

COBIT 5 实施指南中文翻译版

上海汇哲信息科技有限公司

国际信息安全学习联盟

二〇一二年六月

◎汇哲科技声明:

本作品为上海汇哲信息科技有限公司与国际信息安全学习联盟翻译版本,仅供学习交流使用,请勿用于任何商业目的,不得以任何方式修改本作品,请注意对这份文档内容的任何形式的泄露、复制或散布都有可能引起法律纠纷与上海汇哲信息科技有限公司无关。欢迎大家 <http://www.cncisa.com/> 进行讨论和批评指正,我们将真诚的接受你的意见努力改正 guomeng@cncisa.com。

Copyright ©2012SPISEC 版权所有

目录

一、关于我们.....	4
二、引言.....	5
目标和指南适用范围.....	6
三、GEIT 定位.....	8
了解背景.....	8
什么是 GEIT?.....	8
GEIT 为何如此重要?.....	8
GEIT 会交付什么.....	10
综合利用 COBIT5 和集成框架、标准和有效的实践.....	10
原则和成功因素.....	11
四、迈向 GEIT 的第一步.....	12
创建恰当的环境.....	12
运用持续改进的生命周期方法.....	14
阶段 1—什么是驱动程序?.....	14
阶段 2:我们现处于何位置?.....	14
阶段 3:我们想要达到什么位置?.....	15
阶段 4:需要做什么?.....	15
阶段 5:我们怎样才能达到目的?.....	15
阶段 6:我们达到目的了吗?.....	15
阶段 7:如何保持推进的动力?.....	15
导读—确定需要采取的行动: 识别核心问题和触发事件.....	16
典型的核心问题.....	16
内部和外部环境的触发事件.....	17
利益相关者参与.....	18
识别利益相关者的作用和需求.....	19
内部利益相关者.....	19
外部利益相关者.....	20
独立的保证和审计者的作用.....	21
五、确认实施要求和成功因素.....	22
创建适当的环境.....	22
阶段 1:驱动因素是什么?.....	22
阶段 2—我们现处于何位置?.....	24
阶段 3—我们想要达到什么位置?.....	24
阶段 4—我们需要做什么?.....	25
阶段 5—我们怎样才能到达?.....	27
阶段 6—我们到达了吗?.....	28
阶段 7-怎样保持推进的动力?.....	28
六、促进变革.....	30
变革启动的必要性.....	30
GEIT 实施的变革启动.....	31
阶段 1: 建立变革的愿望.....	32

阶段 2: 形成一个有效的实施团队	32
阶段 3: 有效沟通期望的愿景.....	32
阶段 4: 授权任务参与者和确认速效方案.....	32
阶段 5: 促进运营和使用.....	33
阶段 6: 嵌入新的方法	33
阶段 7: 持续.....	33
七、实施生命周期的任务、角色和职责	34
实施生命周期的任务、角色和职责	34
阶段 1-驱动因素是什么?	34
阶段 2-我们现处于何位置?	36
阶段 3-我们想要到达哪儿?	39
阶段 4-我们需要做什么?	42
阶段 5-我们如何到达那里?	45
阶段 6-我们到达那儿了吗?	47
阶段 7-怎样保持改进动力?	50
八、使用 COBIT 5 组件	53
COBIT 4.1, Val IT and Risk IT 使用者的转换注意事项	53
新的 GEIT 原则:.....	53
计划和范围	56
绩效测量	56
治理和管理实践和活动.....	56
角色和职责	57
附录 A:映射核心问题到 COBIT 5 流程.....	57
附录 B:决策矩阵实例	58
附录 C:映射风险情景实例到 COBIT 5 流程.....	62
附录 D:实例业务模式	66
执行概要	66
背景(看第二章, 定位 GEIT)	67
业务难题(看第三章, 第三节, 导读—确定需要采取的行动: 识别核心问题和触发事件).....	67
提议解决方案.....	69
附录 E:COBIT4.1 能力属性表	72
九、联系我们:	73

一、 关于我们

上海汇哲信息科技有限公司（简称“汇哲”或“SPISEC”），总部设立在上海。其前身为业内众多学习群体的持久赞助者；长年致力于信息安全意识、管理、技术、IT 审计、认证等方面的培训和实践研讨，始终以信息安全的共享交流、学习指导、职业规划为己任，并以培养国内信息安全人才、组织中国信息安全专业人员学习交流为发展目标。

SPISEC 为信息安全行业内综合的培训服务模式，重于实践和服务质量的精细、实用，及永久。其讲师均具备信息安全十年以上工作经验，五年以上培训经验，自身长年致力于信息安全培训和服务行业，具备较强的专业培训水平和丰富的培训经验。SPISEC 专业、强大的后续服务团队专为学员解决考试、认证、工作实践等问题。并结合多年培训经验，以培训为基础、服务为保障、实践为目的，为业内企业和个人、业内第三方合作伙伴提供优质的培训服务。

SPISEC 于 2008 年开始在业内陆续组织多场专业知识学习讲座和研讨，并持续发布多期专业原创文档和学习形式期刊、书籍。SPISEC 至今为 20000 多名会员提供免费的学习指导服务，其中为 1500 多名会员直接提供考试辅助、职业规划、学习计划梳理等服务，会员现分布央企、国企、金融、电信、移动、能源、制造、IT 等多个行业。SPISEC 的成立将更好地带动业内信息安全人员的培养和发展，保障国际信息安全学习联盟（www.cncisa.com）的基本运营，实现业内各领域有志之士的共同愿望，汇聚业内各领域的专业顶级人才。

——国内专业唯一的信息安全培训服务商

管理实践类培训服务：

- 信息安全意识培训
- 信息安全风险评估实施培训
- ISO27001 信息安全体系实施培训
- IT 规划实践课程
- IT 治理与信息安全治理实践课程
- IT 服务管理实践课程
- IT 审计实践课程
- 信息安全审计实践课程
- 业务连续性演练计划实践课程
- 企业敏感信息保护实践培训
- 企业定制开发内部培训.....

信息安全认证类培训服务：

- CISA 国际注册信息系统审计师认证培训
- CISSP 国际注册信息安全专家认证培训
- CISM 国际注册信息安全经理认证培训
- CISP 国家注册信息安全专业人员认证培训
- COBIT Foundation 认证培训
- ITILV3 Foundation 认证培训
- CBCP 国际业务连续性管理专家认证培训
- 信息安全管理高级专家认证培训

技术实践类培训服务：

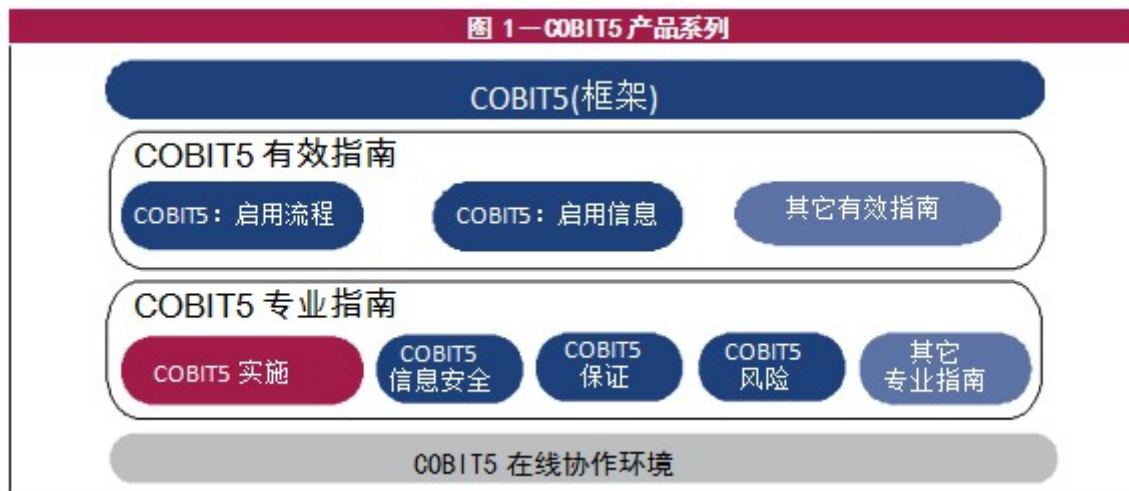
- 网络设备安全技术实践课程
- 信息安全加固和防护实践课程
- 软件开发安全实践课程
- 应用系统安全性评估课程
- 黑客攻击与防范实战课程
- WEB 安全攻防演练课程
- Web 服务器安全培训
- 网络实战攻防技术与安全策略培训
- 企业定制开发内部培训.....

汇哲后续服务保障：

- 专业售后服务部 2 月电话回访
- 公开课学员长年免费复读直到通过
- 每 2 周信息安全通报与学习月刊
- 国际信息安全学习联盟平台支撑
- 定期邮件组和短们平台知识更新
- 长年免费沙龙与实践研讨会
- 每年信息安全免费培训 1 次
- 工作实践与项目支撑免费协助
- 信息安全意识海报和屏保免费

二、引言

COBIT5 实施补充产品 COBIT5(表 1)。这些参考指南的目标就是提供一个为实施 GEIT 的良好实践方法，基于适合特殊企业而定制的持续改进的生命周期。



COBIT5 框架建立了五个基本原理，包括详细说明和包含有关企业 IT 治理和管理保障大量的指南。COBIT5 产品系列包括以下产品：

- COBIT5(框架)
 - COBIT5 保障指南，在治理和管理保障论述得很详细。这些包括：
 - COBIT5:保障流程
 - COBIT5:保障信息(在研发)
 - 其他的保障指南(参考 www.isaca.org/cobit)
 - COBIT5 专业指南，包括：
 - COBIT5 实施
 - COBIT5 信息安全(在研发)
 - COBIT5 保障(在研发)
 - COBIT5 风险(在研发)
 - 其它的专业指南(参考: www.isaca.org/cobit)
 - 在线协作环境，有利于支持 COBIT5 的使用
- 这次发布的内容结构如下：
- 第二章阐明了在一个企业里 GEIT 的定位
 - 第三章描述了迈向 GEIT 的第一步
 - 第四章解析了确认实施要求和成功要素
 - 第五章描述了保障 GEIT 相关组织和行为的变更
 - 第六章详细描述了实施包含变更能力和执行管理的持续改进
 - 第七章描述了使用 COBIT5 和它的组件
 - 一些附录包括：
 - 附录 A 介绍了 COBIT5 流程和流程核心问题的对照
 - 附录 B 提供了决策矩阵范例
 - 附录 C COBIT5 流程风险情况范例对照
 - 附录 D 提供了业务案例的范例

——附录 E 是 COBIT4.1 成熟度表

企业 IT 治理(GEIT)的实施是被高层管理普遍认可的企业治理的重要部分。而当前信息的重要性和信息技术(IT)的普及性正日益成为业务和大众生活方面的部分,需要驱动更多的来自于 IT 投资的价值和管理增加的一系列 IT 相关风险而不会变得更大。越来越多的标准也驱使了董事会之间认识到有效地控制 IT 环境的重要性和必须遵守的法律,法规和合约责任的高度意识。

有效的 GEIT 将会提高经营业绩同时也适应外部要求,而对于很多企业成功实施仍遥遥无期。有效的 GEIT 需要一系列关于针对企业适合的方式和操作规范进行周密规划的角色、职责和责任的保障。这些包含了恰当的文化、行为和指导原理及政策、组织结构且定义明确及管理治理和管理流程,需要决策支持的信息,解决方案和服务的支持,及适当的治理和管理技能。

改进企业 IT 治理已被越来越多的高层管理认识到是企业治理的重要部分。

汇哲科技

多年来 ISACA 已研究企业治理这一主要领域以推进国际思维及提供评价、管理和监控企业 IT 应用的指导。ISACA 已研发了 COBIT5 框架以帮助企业实施健全的治理手段;确实,要实施好 GEIT,没有使用有效的治理框架,几乎是不可能的。最佳实践和标准对加强 COBIT5 基础也是有效的。

框架、最佳实践和标准是有用的,只要企业已采用和适应生效。这是 GEIT 是否实施成功必须战胜的挑战和必须解决的问题要求。董事会和管理层必须得承担更多 IT 的责任,提供原则和框架指导及逐渐传输不同的理念和 IT 价值传递文化。

目标和指南适用范围

在 COBIT5 实施中,重点是整个企业 IT 治理的观念。指南和 COBIT5 认知到在企业中信息和相关信息技术是普及的且它对于各自业务和 IT 相关活动既不可能也不好实施。企业 IT 治理和管理因此会作为企业治理的整体部分实施,覆盖所有业务和 IT 的职责作用域。

本指南也支持包含各种不断增大资源的实施工具组件且 ISACA 会员可从 www.isaca.org/cobit 下载得到。它包含的内容:

- 自评估、测量和诊断工具
- 阐述
- 相关文章和进一步阐述

一些 GEIT 实施为什么失败的一个常见的原因是没开始而且作为真正地确保利益实现的规划进行管理。GEIT 执行需要由高级管理层发起,执行的范围和可达到的明确目标以便企业能获取计划变更的进度。实施管理也因此能访问到实施生命周期的整体部分。

GEIT 执行需要由高级管理层发起，执行的范围和可达到的明确目标。

假定方案和项目的方法足以有效地推动改进计划和措施，目标也建立了‘标准业务实践’和可持续地企业 IT 治理和管理方法，就像企业治理的一些其它方面。由于这些因素，实施方法就是根据授权企业及其利益相关者和任务参与者拥有 IT 相关治理和管理决策所有权及促进活动和有效变更。当 IT-相关优先级和治理改进的重点流程产生可衡量的效益和已经成为嵌入持续发展的业务活动时，实施方案将会结束。

这指南不是一个规范性的方法或完整的解决方案，但相反的指南对避免意想不到的问题、效率平衡是一个最新的良好实践且有助于最后建立成功的治理和管理结果。每个企业会应用自身具体的计划或准则、决策，当然，还有因素如所属的行业和业务环境及自身文化和目标。同样重要事项将是当前启动的核心问题。少数企业没有适宜的 GEIT 架构或流程，尽管他们当前没认识到。因此，重点需要的是创建前企业已经到位了什么，尤其是可采纳的现有成功企业级方法的利用，如果必要，改造 IT 而不是彻底改造不同的东西。另外，一些之前的 COBIT4.1 应用的改进或其它标准及不需要修订的最佳实践，但可能，而必须做的，建立 COBIT5 应用和这个更新的指南作为持续改进的发展部分。

这指南对于熟悉 GEIT 论题的用户和为实施团队能够使用 COBIT5 成功实施 GEIT 拥有必要的专业知识都是有益的。从事相关教育项目将会正确理解 COBIT5 的内容，如何使用 COBIT5 组件和怎样应用实施方法，和 ISACA 提供的包括流程能力评价和基于 COBIT5 的保障活动的其它相关指导一样。ISACA 的企业 IT 治理认证 (CGEIT) 程序也支持这个产品且认可 IT 技能和能力素质的治理。

COBIT5 可通过 www.isaca.org/cobit 网站免费下载。链接到用于实施应用 ISACA 产品的当前页面。

这个指南提供了很多知识和 GEIT 实施的实践经验，应用和使用当前版本和已出来的 ISACA 的 GEIT 指导升级的课程学习。因此 IT 是快速变化的主题，指南的用户也会持续认知 ISACA 的专业化产品和其它组织的标准及已出版的最佳实践有时会访问到新出来的文章。

三、GEIT 定位

了解背景

GEIT 不会发生在真空中。在不同的环境中实施及环境由很多内外部因素决定，如：

- 团体的道德和文化
- 制定的法律、法规和政策
- 国际标准
- 行业实践
- 竞争环境
- 企业的：
 - 宗旨、愿景、目标和价值
 - 治理政策和实践
 - 企业文化和管理方式
 - 角色和职责的数据模型
 - 业务规划和战略目标
 - 经营模式和成熟程度

每个企业的 GEIT 实施由此都不相同，需要了解背景和考虑设计最优的新的或改进的 GEIT 环境。

什么是 GEIT？

术语‘治理’‘企业治理’和‘GEIT’是对于不同的个体和取决于组织的背景的企业，如成熟度、行业和管理环境和人员背景，如工作原理、教育和经验是不同的意思。为该指南其余部分奠定基础，这一节只提供说明，但它会得到已存在的不同观点的认可。最佳方法就是建立和增强包含现有 IT 的方法，而不是只为了 IT 研发一个新的方法。

‘治理’起源于古希腊语中“控制、引导”的意思。治理系统能够实现一个企业多个利益相关者对组织在环境、运营和设定的方向及对企业目标的业绩监测的陈述。建立和维护适当的治理方法是董事会和高级管理层或相同级别的责任。

COBIT5 定义治理为：

治理确保制定评估了利益相关者的要求、条件和运营以确定平衡，认可企业可实现的目标，通过优先处理设定的方向和决策；及业绩监测和对认可的方向和目标的遵守。

GEIT 不是一个孤立的管理，而是企业治理的组成部分。而企业级治理需求主要由交付利益相关者的价值驱动和透明度要求及企业风险的有效管理，重大的机遇，成本和与 IT 专有的相联系的风险，都完整的、集中于 GEIT。GEIT 能够充分发挥 IT 的优势，最大化利益，利用机会而获得竞争优势。

GEIT 为何如此重要？

全世界范围，企业—无论是国有还是私企，大型或小型—日益认识到信息是关键资源而且 IT 是战略

优势及成功的重要促成因素。

IT 成为有助于企业实现最重要的目标的强大的资源。例如，IT 能代表节省大量业务成本的核心驱动，如企业合并、企业收购和企业剥离。IT 也能够进行关键流程的自动操作，如供应链，及新业务战略或业务模式的要素，借以增强竞争力和促进创新，如数字交付产品(如音乐销售和在线交付)。IT 也可以促使与客户更深的密切关系，如通过各类系统中整理与挖掘数据而提供一个 360 度的客户视角。IT 成为缩短地理位置差距的网络经济的基础和提供新的组织氛围及创造价值的创新方式。大多数企业认识到信息和 IT 的应用视为最关键的优势以致需要进行适当的治理。

而 IT 有可能因企业转型，通常会在同一时间作为一个非常重要的投资项目。在很多情况下，真正的 IT 成本不是很透明的且预算遍布业务单元、功能和没有全面监管的地理位置。花费最大的部分通常是‘keeping the lights on’ initiatives(实施后的维护和经营成本)而转型或创新计划。当在战略规划上花费资金时，它们通常未能交付预期结果。许多企业也未能论证具体物，衡量企业 IT 有效投资的价值而 GEIT 的重点是作为处理这种情况的机制。

最新调查发现一系列明确的 IT 和业务成果是 GEIT 实施的结果。

此外，网络经济呈现了一系列 IT 相关风险，如面向客户的业务系统不可用，客户信息或私人数据的泄露，或由于一个不可改变的 IT 体系架构而错失业务商机。这些管理需要和其它 IT 相关风险类型是较好地实施 GEIT 的另一个驱动。

GEIT 的重要性也可以归结为在当今许多行业和区域企业面临的复杂的控制环境，通常延伸的就是直接面对 IT。财务报告的问题和 IT 相关控制的重要性是相一致的问题。

好实践的运用如 COBIT 已授权一些国家和行业，一个例子是土耳其的银行业监管机构(BRSA)，已指令在土耳其经营的所有银行在管理 IT 相关流程时必须采用 COBIT 的最佳实践。在南非一国王III一包含的公司治理报告，第一次用了国际治理标准，实施 GEIT 的原则和建议采用 COBIT 框架。IT 治理框架可以以更有效和高效的方式实现复杂的合规要求。

通过受访者对有关 ISACA 传导的 GEIT 和 PwC 在接下来 12 个月进行检查主要的 IT 相关行动规划的最新调查：

- 46%受访者计划重要的 IT 系统实施或升级
- 45%计划数据和信息行动

这些行动的例子通常有复杂的利益相关者环境(来自于不同业务和 IT 设备的多个利益相关者)就会加强适当的 GEIT 启动的要求。

因此，GEIT 调查发现一系列的 IT 和业务成果都是 GEIT 实施的结果。

- 38%受访者谈到降低了 IT 成本
- 27%体验了一次改进的投资回报
- 42%受访者叙述改进了 IT 相关风险管理
- 28%谈到提高了业务竞争力

调查还显示:

- 大约 47%受访者会一直有效地增强 GEIT 的完善
- 而只有大约 5%受访者表明他们并不认为 GEIT 是重要的, 23%受访者他们仅开始了评估需要做什么
- 29%只有一些临时措施到位

GEIT 会交付什么

本质上, GEIT 与 IT 价值传递到业务及 IT 相关风险缓解相关。这有效促进了可用性和充足资源的管理及绩效测量到流程监测走向预期的目标。

GEIT 关注以下目标:

- 利益实现——通过 IT 创造企业新价值, 保持和从现有的 IT 投资增加价值和削减不能为企业创造足够价值的 IT 行动和资产。IT 价值的基本原则是提供适合目的的服务和解决方案, 按时且在预算范围内及产生经济而非经济的预期效益。IT 交付的价值将会直接调整有关集中的业务和透明显示效果的测量方式和企业 IT 投资的价值创造过程的贡献的价值。
- 风险优化——解决业务风险与使用、所有权、操作、参与、影响和企业采用的相关。会极大地影响业务的 IT 相关事件构成了 IT 相关的业务风险。而价值交付关注的是价值创造, 风险管理关注的是价值的保持。IT 相关风险的管理将会集成在企业风险管理方式中以确保企业 IT 的重点且以显示效果的透明方式测量及 IT 相关业务风险优化在价值保持的作用。
- 资源优化——确保适当的能力以执行战略规划和充分性, 适当性和有效性的资源提供。资源优化确保提供一个完整的、经济的 IT 基础设施, 为业务需求引进技术, 更新和替换淘汰的系统。它强调了人, 还有硬件和软件的重要性, 因此, 重点是提供培训, 晋升留用及确保关键 IT 人员的专业能力。

战略调整和绩效测量也很重要且涉及到所有的活动以确保 IT 目标与企业的目标相一致。

综合利用 COBIT5 和集成框架、标准和有效的实践

董事会应授权采用和适应 GEIT 的框架, 如 COBIT5 是一个企业治理发展的完整部分。当设计具体的政策, 流程, 技术和程序时, 框架提供了整体的方法且由具体的标准和可以使用的良好实践提供指导。

通过框架间的工作和利用有效的实践, 适当的治理流程和其它已研发和优化的手段, 以便 GEIT 作为通常的业务实践有效地运行且有支持的文化, 通过高级管理层展示。采用 COBIT 也会产生较快和更有效的外部审计, 因为 COBIT 是受到广泛认可作为 IT 审计程序的基础。

董事会和高级管理层应授权采用 GEIT 框架作为企业治理的完整部分。

框架和由此引起的调整内容和以下的内容协调一致（除了其它的）：

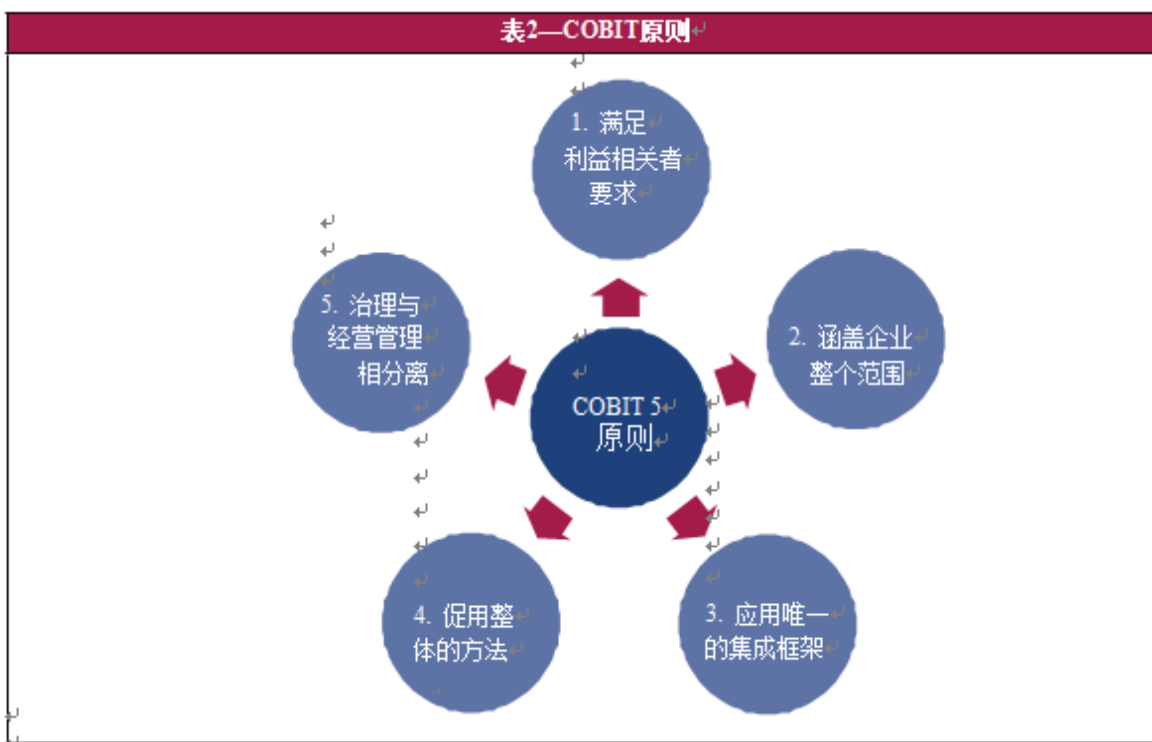
- 企业的政策、策略、治理和业务规划及审计方法
- 企业和风险管理 (ERM) 框架
- 现有企业的治理组织、结构和流程

COBIT5 适用于各种类型和规模的企业，包括非营利组织和公共机构，目的是交付企业的商业利益，包括：

- 增加运用 IT 创造的价值；IT 保障和服务的用户满意度，降低 IT 相关风险；且遵守法律、法规和合约要求。
- 更多业务集中的 IT 解决方案和服务的发展。
- 增加整个企业参与 IT 相关活动。

原则和成功因素

COBIT5 是基于五个原则和七个成功因素。COBIT5 明确的原则内容如表 2



成功因素应被视为有助于促进企业框架目标和价值交付的实现：

- 原则、政策和架构
- 流程
- 组织的结构
- 企业文化、道德规范和行为
- 信息
- 服务、基础设施和应用
- 人、技能和职业能力

COBIT5 包括的进程有助于指导治理和管理手段的建立和维护：

- EDM01 确保治理框架建立和维护（企业文化、道德规范和行为；原则、政策和架构，组织的结构和流程）
- AP001 管理 IT 管理框架（企业文化、道德规范和行为；原则、政策和架构，组织的结构和流程）
- AP003 管理企业的架构（信息；服务、基础设施和应用）
- AP007 管理人力资源（人、技能和职业能力）

COBIT5 治理和管理流程确保了企业以重复的和可靠的方式组织它们的 IT 相关活动。COBIT5 流程参照模型，分为 5 个域和 37 个流程构成了详细的 COBIT5 流程指南结构，在 COBIT5 的保障流程中详细描述。

COBIT 5 是基于企业视角且与企业治理最佳实践保持一致，推动 GEIT 作为更广泛的企业治理的一个组成部分实施。COBIT5 也提供了一个有效整合其他架构、标准和实践应用，如信息技术基础架构库 (ITIL), 开放式企业架构 (TOGAF), 国际标准化组织 (ISO) / 国际电子委员会 (IEC) 27000 的依据。它和 GEIT 标准是相一致的，ISO/IEC 38500:2008, 它阐明了高级别的 IT 治理原则，涵盖了职责、战略、获取、性能、遵守和治理机构的人员行为，如董事会，应评估，指导和监督。COBIT5 是一个总体框架，作为非技术的，没有技术知识的通用语言的统一和完整的指导来源。

四、迈向 GEIT 的第一步

创建恰当的环境

当实施 GEIT 改进时，已有的适当环境是很重要的。这有助于确保行动本身是可治理的且充分地指导和支持管理。多数的 IT 行动通常是由于不成熟的管理指导，支持和监督。GEIT 实施是不同的，如果治理好和管理好，他们会有更多的成功机会。

企业 IT 治理的实施管理应明确和规划指导原则，决策权，职责框架。

主要利益相关者不充分的支持和指导可能会，如导致 GEIT 行动产生没有适当所有权新的的政策和程序。没有一个分配角色和职责，致力于持续经营，符合性监督的管理机构，流程改进是不可能成为标准的业务实践。

因此而建立和维护适当的环境将确保 GEIT 作为一个企业内部全面治理方式的整体部分实施。这将包括适当的指导和实施行动的监督，包括指导原则。其目的是提供充分的保证，指导和控制活动，以便与企业的目标保持一致及董事会和高级管理层的适当执行支持。

许多情况的经验表明，GEIT 行动在全面的企业治理中识别了重大的弱点。GEIT 很难在一个差的企业治理环境获得成功，因此高级管理人员的积极支持和参与更为重要。董事会应意识到需要改进整体治理和如果没有这样的参与就会有 GEIT 失败的风险。

无论完成的是小的或主要的行动，高级管理层都必须参与和推动合适的治理结构的建立。最初的活动通常包括当前实践的评估和改进结构的规划。一些情况下它可能会导致业务重组，IT 功能和与业

务单元相联系的也一样。

高级管理层应建立和维护治理框架—这意味着确定结构，流程和符合规定的治理设计原则，决策模型，管理水平和提供决策模型所需的信息的 GEIT 实践。
高级管理层还应为指导 GEIT 改进计划分配明

使 GEIT 有效的最好方法之一，提高高级管理层和董事会的视角，并确定企业 IT 活动的方向以设立一个 IT 执行战略委员会。

使 GEIT 有效和为高级管理层和董事会提供一种机制及 IT 相关活动指导的最佳方法之一是设立 IT 执行战略委员会。该委员会的作用在于代表董事会(承担责任的)及负责企业 IT 应用情况和作出影响企业的关键 IT 相关决策。它将有明确界定的权力，且最好由企业高级管理层担任要职(理想的是董事会成员)和由代表主要业务单位的高级企业管理人员，以及首席信息官(CIO)，如果需要，还有其他高级 IT 经理组成。内部审计和风险功能应提供咨询作用。

高级管理层需要基于业务和 IT 经理、审计师及其他人员的各种观点作出决策。COBIT5 框架有利于通过提供一个通用语言为高级管理层沟通目标，经营目标和预期结果。

表 3 和表 4 当建立了适当的环境以维持治理和确保成功的结果时，说明例子中主要利益相关者的一般角色和实施任务参与者的职责。在下一节介绍的实施生命周期的每一阶段都提供了类似的表。

表 3—在创建适当的环境中角色	
当你是……	在创建适当的环境中你的角色是……
董事会和高级管理层	建立方案的方向，确保与企业治理和风险管理保持一致，审批关键方案的角色和明确职责，且给予可视的支持和保证，发起人，传达和推动一致的行动。
业务管理层	提供适当的利益相关者和提倡者以驱动保证和支持方案，指定关键方案的角色和定义及分配职责。
IT 管理层	确保业务高级管理层了解和重视高难度的 IT 相关问题和目标；指定关键方案的角色和定义及分配职责，指定人员驱动业务协议方案；
内部审计	决定的作用和报告审计参与的准备工作，确保提供审计参与的适当程度贯穿于方案期间。
风险,遵守和合法	确保足够的参与程度贯穿于方案期间

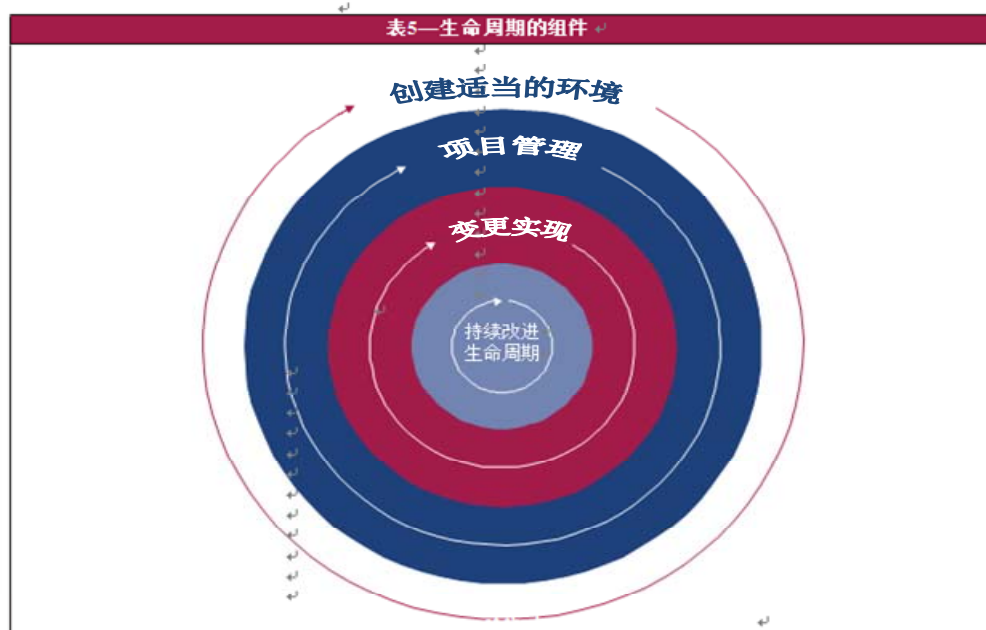
表 4—创建适当环境RACI图									
主要的活动		实施任务参与者的职责							
		董事会	IT执行委员会	首席信息官(CIO)	业务执行经理	IT经理	IT流程所有者	IT审计	风险和合规
设定项目的方向。		A	R	R	C	C	I	C	C
提供项目管理资源。		C	A	R	R	C	C	R	I
建立和操持方向及监督结构和流程。		C	A	C	I	I	I	I	R
建立和维护项目。		I	A	R	C	C	I	I	R
保持与企业一致的方法。		I	A	R	C	C	I	C	R
RACI图明确了执行，负责，商议或告知的活动任务分配。									

运用持续改进的生命周期方法

运用持续改进的生命周期方法可以为企业提供了方法以处理 GEIT 实施期间错综复杂的事物和通常遇到的难题。生命周期有三个相关的组件，如表 5 中在图解：GEIT 持续改进生命周期的核心部分，变更的实现（解决实施或改进的行为和企业文化方面问题）和项目管理。在表 5 中，描述持续生命周期的措施强调的是标准过程而不是一次性的活动，但实施和改进的持续流程部分最后实现了“一切照常”这时项目就可以结束了。

实施生命周期的七个阶段在表 7 中说明。实施和改进项目通常是持续和重复的。在最后阶段，确定了新的目标和需求时，新的周期又将开始了。

高级稳健的检查、评估和审计是在 GEIT 最初阶段触发而这些结果会运用于输入阶段 1。



阶段 1—什么是驱动程序？

阶段 1 确定当前改变的驱动程序和创建描述这种改变的行政管理水平，然后陈述出企业情况的概要。一个改变的驱动程序是内部或外部事件，环境或促进改变的主要问题。事件、趋势（行业、市场和技术）、性能不足、软件实施，甚至企业的目标都可能会成为改变的驱动。与项目实施自身相关的风险应在企业情况中描述，而管理应贯穿于整个生命周期。筹备、维护和监督企业情况是基础和调整、支持的重要管理，以及确保一些行动的成功结果，包括 GEIT 的实施。它们确保持续关注项目的收益和实现。

阶段 2:我们现处于何位置？

阶段 2 保持 IT 相关目标与企业战略和风险目标相一致，且优先处理企业最重要的目标，IT 相关目标和流程。COBIT5 提供企业目标到 IT 相关目标及 IT 流程的通用对照表，有助于进行选择。确

定了已知的企业和 IT 相关目标，关键的流程后需要有足够的能力去确保成功的结果。管理者需要了解企业目前的能力和可能存在的缺陷。这是通过流程能力评估选定对象过程的现有状况实现的。

阶段 3: 我们想要达到什么位置？

阶段 3 设定改进的目标，继而进行差距分析以确定可行的解决方案。一些解决方案会是速效的，而更多的是艰巨的、长期的任务。应优先考虑那些容易实现和可能产生最大效益的项目。长期的任务应分解为便于管理的块。

阶段 4: 需要做什么？

阶段 4 计划切实可行和实用的解决方案具有明确的项目支持和可行的业务情况，且制定实施改变的计划。一个成熟发展的企业情况有助于确保可确认和持续监督的项目效益。

阶段 5: 我们怎样才能达到目的？

阶段 5 提供实施的解决方案纳入日常实践中和建立措施和监督系统以确保业务目标的实现和可衡量的绩效。成功需要最高管理层和所有受影响的业务及流程所有者的参与、意识和沟通，了解及保证。

阶段 6: 我们达到目的了吗？

阶段 6 关注改进治理的可持续转变和管理实践纳入正常的业务经营及运用绩效测量和预期效益来监测改进的完成。

阶段 7: 如何保持推进的动力？

阶段 7 回顾整个成功的行动，确定进一步的治理或管理需求且增强持续改进的要求。它也优先考虑进一步提高 GEIT 的机会

方案和项目管理是基于有效的实践且在七个阶段的每一阶段都提供了检查点以确保方案的执行步入了正轨，业务情况和风险的改造，且为调整下一阶段规划得更恰当。理论上应遵循企业的标准法。方案和项目管理的进一步指导也可在 COBIT5 流程 BAI01 中看到。尽管文章没有明确提及在哪个阶段，但它是一个持续的贯穿于所有阶段且是重复的。

每个阶段花费的时间有很大的不同，取决于(除其它因素外)具体企业的环境，它的成熟度，和实施的范围或改进的行动。然而，随着改进应用的日益增加，整个生命周期总体花费的时间理论是应不超过六个月；另外，也有失去推进力和来自利益相关者关注和认可的风险。目标是进入一个有节奏的规律的改进。较大规模的行动应是结构为多个迭代的生命周期。

随着时间的推移，生命周期随之应是反复的，直到建立了可持续的方式。当生命周期的阶段成了每天的活动且持续改进自然发生时，它就成了标准的企业实践。

导读—确定需要采取的行动：识别核心问题和触发事件

很多因素表明了需要新的或改进的 GEIT 实践。然而，重要的是注意这些特征，不只是指出潜在的问题，但也可指出其它的问题(或组合因素)。例如，如果企业对 IT 成本高得不可接受有看法，这也许是由于治理和/或管理的问题(IT 投资管理流程应用了不适当的标准)，但它也会因为过去 IT 的投资不足，现在出现重大的投资需求。

通过应用核心问题或触发事件作为企业 IT 治理行动的启动点，GEIT 改进企业状况也与有经验的事宜相关，它会提高对商业案例的认可。企业内建立的紧迫感是必须启动实施。另外，已确定的速效和已论证的区域价值增进是企业内最可见或认可的。它为提出更进一步的改变提供了一个平台且有助于获得高级管理层对更深入的改变的更为广泛的保证和支持。

通过应用核心问题或触发事件作为企业 IT 治理行动的启动点，GEIT 改进企业状况也与有经验的事宜相关，它会提高对商业案例的认可。

典型的核心问题

新的或改进的 GEIT 实施通常解决或部分解决以下症状：

- **业务受挫由于失败的措施、IT 损失的风险和低业务价值的认知**
——当许多企业持续增加他们的信息科技投资时，这些投资的价值和 IT 的整体性能通常存在问题或未完全实现。这也是 GEIT 问题表现出来的 IT 和业务之间需要加强沟通和 IT 的作用和价值的共同看法需要建立。这也是不理想的投资组合和项目规划、方案和审批机制的结果。
- **与 IT 相关业务风险有关系的重大事件，比如数据丢失或项目失败**
——这些重大事件通常只是冰山一角且如果受到公众和/或媒体的关注会加重影响。进一步的调查往往导致更深入的鉴别和结构失调或更甚的企业内完全缺乏 IT 风险意识的企业文化。强大的 GEIT 实施这时就要求获得完全的视角和实际了解 IT 相关风险及它是怎样进行管理的。
- **未能满足规范管理和合约需求**
——在许多企业，无效率或无效果的治理机制阻碍了有关法律，法规和合同条款作为整体纳入组织的系统或缺乏一个管理它们的方法。全世界范围内普遍增加的合规和合法需求通常随着 IT 促进活动的影响而增加。
- **企业的创新能力和业务迅速发展受到 IT 的制约**
——普遍抱怨的是在有以提供竞争力创新能力的的需求时，IT 支持功能的作用不足。一些症状可能指业务和 IT 之间缺乏真正的双向调整。这也许是由于在战略规划和业务驱动行动阶段 IT 参与业务得太迟。当经济环境要求企业迅速作出响应如新产品或服务的推出时，这问题通常是最突出的。
- **定期的审计发现关于不足的 IT 性能或提到的 IT 服务质量问题**
——这也许是服务水平不到位或不正常，或在 IT 决策制定时参与业务不足的象征。
- **隐藏的或欺诈的 IT 支出**
——缺乏足够透明或 IT 支出及投资的全面观点。IT 支出通常被“隐藏”在业务单位预算中，或没有对 IT 支出帐目进行分类，创建一个总体上存在偏见的 IT 成本的视角。
- **重复或交叉的行动或浪费资源**

- 这通常是由于缺乏一个资产投资组合/所有 IT 行动的整体视角并表明了围绕资产投资组合的流程和决策结构的能力及性能管理的不到位。
- **IT 资源不足, 人员技能不足或人员精力不足/不平衡**
——效能监督要求足够的 IT 人力资源管理问题和确保人员管理的有效的治理及有效解决技能的发展。这也表明了(除其它因素外)IT 需求管理和内部服务交付应用的根本弱点。
 - **为满足业务要求的 IT 有效变更频繁失败和交付迟或超出预算**
——这些核心问题都与业务-IT 定位, 明确的业务需求, 效益实现过程, 或未达标的实施和项目/方案管理流程的问题有关系。
 - **多重的和复杂的 IT 保证投入**
——这可能表明了业务和 IT 有关要求与实行的 IT 相关保证方案不协调。最明显的情况可能是对 IT 依赖的低水平企业, 造成企业实施自身的方案, 或缺乏适当的 IT 保证方案的企业责任, 导致在发生时未有察觉。
 - **董事会成员, 执行层或高级管理层勉强参与 IT, 或缺乏对 IT 业务保证的承诺和满足**
——这些核心问题通常与企业缺乏对 IT 的了解和领悟, 缺乏 IT 在适当水平的能见度, 缺乏管理结构, 或与董事会执行有关的问题有关系, 通常会造成业务和 IT 之间缺少沟通和对于 IT 业务保证中业务和 IT 的误解。
 - **复杂的 IT 运营模式**
——复杂的本质在于, 例如, 分散式的或集中式的 IT 组织通常有不同的结构、应用和政策要求加强关注 GEIT 以确保最优 IT 决策制定和有效的和高效的运营。指的这一问题随着全球化变得更为重要因为每个区域或地区都有需要解决的具体的和可能唯一的内部或外部环境因素。

内部和外部环境的触发事件

除了之前描述的症状外, 企业的内部和外部环境的其它事件, 如下, 会指明或触发关注 GEIT 且在企业议事日程驱动 GEIT:

- **并购、收购或剥离**
——战略上的和经营上的成果与 IT 可能对并购、收购或剥离有效有关系。在尽职调查方案期间需要获得在这种环境 IT 问题的了解。而且, 在这之中的所有其它的企业合并或重组要求, 这都需要设计到适当的新环境的 GEIT 方法中。
- **市场、经济和竞争地位的变化**
——例如, . 经济衰退可能导致企业修改 GEIT 方法以使大规模的成本优化或性能提高。
- **业务操作模式的改变或资源配置**
——例如, 从分散的或集中的模式向更为集中的操作模式迁移将需要改变 GEIT 的实施以保证更为集中的 IT 决策制定。另一例子是共享区域服务中心的实施, 如财务、人力资源或采购。这可能会受到 IT 影响, 如独立的 IT 应用的整合或基础设施功能域需要进行相应的改变已治理的 IT 决策结构或流程。一些 IT 功能和业务流程的外包同样也会导致 GEIT 的问题。
- **新法规或合法要求**
——举个例子, 增大了公司治理报告要求和金融法规触发了改进 GEIT 的要求和普遍由 IT 引起的信息保密性问题。
- **重要的技术变更或模式转换**
——一个例子是企业从面向服务的体系结构(SOA)向云计算的迁移。这从根本上变更了基础设施和应用功能的开发和交付方式, 也会要求变更相关的流程方式及治理和管理的其它因素。
- **企业的治理重点或方案**

——这个方案将会触发启动的 GEIT 范围。

- **新的首席信息官(CIO)、首席财务总监(CFO)、首席执行官(CEO)或董事会成员**

——新任命的 C 级别的官员通常会触发目前 GEIT 机制的评估和启动解决发现的薄弱环节。

- **外部审计或咨询评估**

——由独立的第三方对适当的实践的评估通常是 GEIT 改进行动的启动点。

- **新的经营战略或重点**

——追求新的经营战略会对 GEIT 有影响。例如：接近客户的经营战略…等，知道他们是谁，他们的需求和应对这些需求可能的最佳方法—可能需要更自主的业务单位/地区的 IT 决策而不是企业或支持层面的重要的决策。

- **期望有效地提高 IT 投资价值**

——提高竞争优势需要：创新、资产优化、或创造新的商业机会都会引起 GEIT 的注意。

需要采取的行动应得到确认和广泛征求及沟通。这种沟通既可以是“非正式的”（讨论重点在哪）方式也可以是实行的改进时机和效益实现的书面表达。目前 GEIT 的重点或触发事件提供了启动点—确定这些通常是通过高级安全检查、诊断或能力评估来完成。这些技术有助于在解决问题上建立增进效益的共识。它也有益于第三方对当前现状执行审查以获得独立的和客观的高水平评价，也会加大对采取行动的支持。

还有一个是需要争取董事会和执行管理层从一开始就提供的保证和支持。为了做到这，GEIT 的方案和目标及效益应在企业方案中明确表达。逐步灌输改正的迫切程度，且董事会和执行管理层应意识到有效治理和 IT 管理给企业带来的价值以及不采取行动带来的风险。这也确保 GEIT 方案和企业目标和战略目标和企业 IT 目标及和企业治理保持一致，而 ERM 行动（如果已经存在）视为开始。一些速效的确定和实现（现有的问题可以得到相对快速地解决且有助于通过显著的效益证实整体行动确实有效）也是获得董事会保证的一种有用的方法。

一旦高层设立了方向，应实现各层级的整体视角的变革启动，更大规模和范围的变更首先需要了解艰难的商业条件，其次是来自人和行为的视角。需要确定所有参与或受变革影响的利益相关者及确认其相对变革的位置。2011 年 GEIT 调查显示变革启动可能是实施 GEIT 的最大挑战之一：38% 的被调查者提到变革管理视为挑战，而 41% 叙述为沟通问题。变革的关键动因是企业 and IT 管理者促进 GEIT 实施动机的确认。

利益相关者参与

许多利益相关者需要共同协作来实现改进 IT 性能的整体目标。COBIT5 是基于利益相关者的需要和方法提供了本指南，将有助于建立一个商定的和普遍理解的需要获得什么以满足利益相关者关心的同等重要的事和协调方式。最重要的利益相关者和他们关心的是：

董事会和高级管理层

——如何设定和明确企业 IT 应用和相关建立的监控及 GEIT 启动需求的方向，以便交付企业价值和降低 IT 相关的风险？

业务执行经理、IT 管理和业务流程所有者

——如何促成企业确定/调整 IT 相关目标以确保交付企业价值和降低 IT 相关的风险？

业务经理、IT 管理和业务流程所有者

——怎样计划、建立、交付和监控信息和 IT 结果和业务需求的服务能力及董事会的方向？

风险、合规和法律专家

——如何确保我们是遵守政策、法律、法规和合约，且风险可识别、评估和减低？

内部审计

——怎样提供有关价值交付和风险缓释的独立性保证？

实施的关键成功因素？

- 高级管理层提供方向和任务
- 所有各方了解企业和 IT 相关目标
- 有效的沟通和必要的组织上的和现有流程变革的启动
- 定制适合企业的目的和规划的框架和有效实践
- 初期的焦点是支持流程和最有益的改进事宜的优先处理是最易于实施论证优势和创建有把握的增进改进

识别利益相关者的作用和需求

内部利益相关者

在图 7 中，综述了内部利益相关者，他们最重要的高层次的职责和义务在于改进流程，而他们感兴趣的是提供的实施方案的结果。这些代表通用的实例。因此，将需要一些适应变化、扩展和定制化服务。

图 7—内部 GEIT 利益相关者的综述

内部利益相关者	重要的高层次的职责和义务	感兴趣的实施方案结果
董事会和高级管理层	为实施方案设立整体方向、环境和目标且确保与企业业务战略、治理和风险管理相一致。为方案提供能见的支持和承诺，包括发起者的作用和促进措施。审核方案的结果，且确保达到预期的利益和采取适当的改进措施。确保需求资源(财务、人力和其它)可用于新的措施。在高层设立方向和以身作则。	董事会和高级管理层感兴趣于从实施方案中获得最大化的业务收益。他们想确保所有相关的需求问题和领域得以解决，开展的需求活动和预期结果能成功交付。
业务管理者和业务流程所有者	为核心实施团队提供适当的业务资源。与 IT 合作以确保改进方案的结果是一致的且适用于企业的业务环境及交付价值和管理风险。能见的支持改进方案 and 与 IT 合作解决一些问题是有经验的。确保在实施和应用的变革期间业务的充分参与。	这些利益相关者希望方案结果能更好地定位调整 IT 与整体业务环境及他们的具体领域。
CIO(首席信息官)	提供方案的领导作用和核心实施团队的适当的 IT 资源。与业务管理者合作和为方案管理设置	CIO 希望确保所有的 GEIT 实施目标得以实现。对于 CIO，

	适当的目标、方向和方法。	方案将导致持续改进的业务关系,调整的业务(包括对 IT 性能的共同看法),IT 支持和请求的最佳管理及改进的 IT 相关业务风险管理的机制。
IT 管理者和 IT 流程所有者,如操作主管,首席设计师,IT 安全管理者,业务持续性管理专家等	为方案和实施团队资源的工作流提供领导作用。把关键的投入放到当前的性能评估中和为各自请求的流程领域设立改进的目标。应结合相关的有效实践提供信息和提供专业建议。确保业务实例和方案计划是切合实际和可实现的。	这些利益相关者对确保改进措施结果能更好地治理 IT 整体和它们独自的领域感兴趣。业务投入需要这样做是获得的最好的可能的方式。
合规、风险管理和法律专家	根据需要参与整个方案和提供合规、风险管理和相关问题的法律信息。确保与总体 ERM(企业风险管理,如果已有)方法相一致和确定相关的法规和风险管理已符合,问题已考虑和收益已获得。在实施期间根据需要提供指导。	这些利益相关者希望确保新的措施处于的位置或对于确保法律和合约履行还有 IT 相关风险管理的有效的改进机制,而且这些与可能存在的一些企业的方法是相一致的。
内部审计者	根据需要参与整个方案和提供相关问题的审计信息。提供有关当前已经历问题的建议和有关控制措施和方法的投入。审查业务实例和实施计划的可行性。在实施期间根据需要提供指导。一个潜在的作用是还可以独立的验证评价结果。	这些利益相关者对实施方案有关的控制措施和方法的结果感兴趣,且建立或改进怎样的机制将会促进当前审计结果得以处理。
实施团队(联合的业务和 IT 团队,由来自之前的利益相关者分类的人员组成)	方向、设计、控制、驱动和执行端到端方案从目标和需求的确认到方案对业务目标的结果评价及确认新的启动和促进实施的目标或改进周期。确保在变革期间从实施环境到操作、使用和维护环境技能的转换。	团队希望所有 GEIT 计划的预期结果铁得以实现和最大化。
员工	支持 GEIT	这些利益相关者对措施将会影响到他们日常工作、角色和职责及活动感兴趣

外部利益相关者

除了列在图 7 中的内部利益相关者外,还有几个外部利益相关者。而这些利益相关者在实施方案中没有任何直接的职责和责任。他们可能有些需要满足的需求。图 8 呈现了通用的实例。

图 8—外部 GEIT 利益相关者实例

外部利益相关者	感兴趣的实施方案结果
IT 服务供应商	企业管理将确保在企业全面 GEIT 和他们提供的服务治理和管理之间有个调整 and 对接。
监管者	监管者对实施方案结果是否满足和/或提供的架构和机制满足所有适用的法规且符合要求感兴趣。

利益相关者(相关的)	利益相关者可能部分基于企业治理状况的投资决策和在这领域它的跟踪记录。
客户	客户可能会受到 GEIT 目标满足程度的影响。一个实例是 IT 相关业务风险管理。是否会暴露企业的安全功能域，如由于丢失了客户的银行数据，客户就会受到影响。客户不直接对实施方案的成功结果感兴趣。
外部审计者	外部审计者可能会评价更多信赖 IT 相关控制作为有效实施方案的结果且会对合规方面和财务报告感兴趣
业务合作伙伴，如供应商等	与企业使用自动化电子交易的业务合作伙伴会对实施方案的结果有兴趣，因为涉及到提高信息的安全性、完整性和及时性。他们也会对合规和国际标准认证感兴趣，可能是方案的结果。

独立的保证和审计者的作用

IT 管理者和利益相关者需要意识到保证专家的作用——他们可能是内部审计者，外部审计者，ISO/IEC 标准审计者，或一些受托提供 IT 服务和流程保证的专业人员。日益的，董事会和高级管理层会寻求独立的建议且作为关键 IT 功能和服务的鉴定。还有普遍增加必要的遵守国家和国际法规的论证。

五、 确认实施要求和成功因素

来自 GEIT 实施的成功经验显示可能有几个实际问题需要解决为了新措施的成功和持续改进的延续。这一章描述了这几个难题以及可能的根本原因和应考虑的因素，以确保成功的结果。

创建适当的环境

阶段 1:驱动因素是什么?

图 9 列出了在阶段 1 中的问题和根本原因及成功因素。

图 9—阶段 1:驱动因素是什么?	
问 题	<p>缺少高级管理层的认同、承诺和支持</p> <p>难于展示价值和效益</p>
根本原因	<ul style="list-style-type: none"> ● 缺乏企业改进治理的重要性、紧迫性和价值的理解(和根据) ● 缺少 GEIT 范围和 IT 治理与管理之间差异的了解 ● 实施对问题的短期反应驱动了实施，而不是提前行动，广泛的改进理由 ● 担心“又一个项目可能会失败的”——缺乏对 IT 管理的信任 ● 缺少治理问题和收益的有效沟通——收益和时间框架没有明确地衔接 ● 没有高级管理层愿意做保证人或负责 ● 只有执行经理相信 GEIT 是 IT 管理的职责 ● 没有合适的团队(角色参与者)承担 GEIT 责任或缺乏适当的技能承担任务 ● 不知道框架的用法/缺少培训和认知 ● GEIT 在当前企业治理环境的不正确定位 ● 计划驱动热衷于传道书本方法的“转换”
成功因素	<ul style="list-style-type: none"> ● 形成 GEIT 董事会、审计委员会和风险委员会讨论会的议事项目 ● 建立一个委员会或利用现有的委员会，如 IT 执行战略委员会提供活动的授权和问责制 ● 避免形成 GEIT 似乎是“查找问题”的结果——必须是一个真实的需求和潜在的收益 ● 确认和沟通可能激发改变现状要求的核心问题 ● 使用适合大众的语言、方法和通信——避免他们不认识的行话和术语 ● 联合(与业务)明确和达成一致 IT 预期价值 ● 传达(一致)业务条款/衡量标准体系的优势 ● 获得，如果需要，支持，和提高技能，外部审计师或咨询和顾问 ● 研究指南原则建立变革投入的定调和场景 ● 基于企业变革投入细目产生规则，为成功建立必要的信任和合作 ● 基于战略重点和当前企业核心问题优化和调整业务实例 ● 获得 GEIT 事宜和框架的学习和培训

问 题	<p>难于得到所需业务的参与</p> <p>难于确认利益相关者和角色参与者</p>
根本原因	<ul style="list-style-type: none"> ● GEIT 没有业务主管的优先权(没有一个关键的绩效指标[KPI]) ● IT 管理偏好独立工作——表明之前涉及“客户”的概念 ● IT 与业务之间禁止参与的障碍 ● 对于业务参与没有明确的角色和职责 ● 关键业务人员和影响者没有参与或忙碌 ● 业务主管和流程所有者了解 GEIT 收益和价值有限
成功因素	<ul style="list-style-type: none"> ● 促进高层管理者和 IT 执行战略委员会建立授权管理和督促 GEIT 中的业务角色和职责 ● 提出一个吸引利益相关者参与的过程 ● 清晰地说明和宣传利益 ● 解释不参与的风险 ● 在改进 GEIT 中作为业务参与的领导人/典型识别关键的服务或主要的 IT 措施 ● 找到信任者——认知良好 GEIT 价值的业务用户 ● 促进自由想法和权力下放，但只是在定义明确的政策和治理结构中。 ● 确保那些责任和需要驱动变革的人是获得承诺支持的那些人。 ● 创建业务参与的讨论会——如 IT 执行战略委员会——主持专题讨论会公开讨论当前问题和改进的机会。 ● 包含业务代表在内的高水平当前情况评估
问 题	在 IT 管理中缺乏对业务的深刻理解
根本原因	<ul style="list-style-type: none"> ● IT 领导只有运营技术背景——参与企业业务问题不够 ● IT 管理在企业中是独立的——没有参与到高一层级 ● 差的业务关系流程 ● 理解业绩不佳的遗留问题驱动 IT 和 CIO 为运营保护模式？ ● CIO 和 IT 管理处于弱势位置，不愿意揭示内部弱点
成功因素	<ul style="list-style-type: none"> ● 通过依靠成功建立可信任度和 IT 员工受敬的绩效 ● IT 管理者理念上应是执行委员会长久的成员之一以确保 IT 管理者具有足够的业务理解和更早地参与到新的计划措施中。 ● 实施有效的业务关联流程 ● 邀请业务参加和参与。考虑 IT 中安排业务人员亦能获得经验和增进沟通。 ● 如果必要，改编 IT 管理角色和与其它业务职能部门建立正式的联系，如财务、人力..... ● 确保 CIO 具有业务经验。考虑从业务中任命一位 CIO ● 使用顾问创建更强大的以业务为导向的 GEIT 战略 ● 建立治理机制，如业务关系经理和 IT，以促进更大的业务视角。
问 题	<p>缺乏当前企业政策和指导</p> <p>差的当前企业治理</p>
根本原因	<ul style="list-style-type: none"> ● 委员会和领导作用问题，可能由于组织的不成熟

	<ul style="list-style-type: none"> ● 专制的文化，基于个人指令而不是企业的政策 ● 文化提升的自由想法和非正规化的方法而不是一个'控制环境' ● 差的企业风险管理
成功因素	<ul style="list-style-type: none"> ● 提出问题和引起董事会级别的高级管理层，包括非高级管理层的关注：缺少治理的风险，基于真实的问题关系到合规性和企业的效益。 ● 提出问题到审计委员会或内部审计 ● 获得外部审计师的支持和指导 ● 考虑文化可能需要怎样的改变以促进提高治理应用 ● 确保整个企业应用了风险管理

阶段 2—我们现处于何位置？

阶段 3—我们想要达到什么位置？

图 10 列出了在阶段 2 和阶段 3 中的问题和根本原因及成功因素。

图 10—阶段 2：我们现处于何位置？和阶段 3—我们想要达到什么位置？	
问 题	缺少高级管理层的认同、承诺和支持 难于展示价值和效益
根本原因	<ul style="list-style-type: none"> ● 行动的理由不明确或不存在 ● 充分证明需求投资(成本)的预知收益失败 ● 担心由于变革丧失生产力或效率 ● 对改进目标缺乏明确的保证和承诺责任 ● 业务从战略参与到技术和运营水平缺乏适当的架构 ● 不适当的沟通方式（没有保持一种简单的，没有使用简洁的和业务的语言，不适合政治和文化）或不适应风格不同的群体 ● 业务状况的改进不先进或不清楚表达 ● 在变革启动和获得所有要求级别的支持中的不足问题
成功因素	<ul style="list-style-type: none"> ● 形成对提高 GEIT 价值一致的认识 ● 具有适当的架构，如：IT 战略委员会、审计委员会、以促进目标的沟通和协商和建立会议制度以交流战略状况、彰明不理解的内容和分享信息 ● 实施有效的业务关联流程 ● 形成和执行变革启动战略且沟通计划说明需要达到更高的成熟度水平 ● 用正确的语言和通用的术语适对象群的风格（使它有趣，使用可视效果） ● 发展最初的 GEIT 业务状况为详细的具体的改进的业务状况，具有清晰的风险描述。关注业务增加的价值（用业务术语表示）以及成本。 ● 教育和培训 COBIT5 和实施方法
问题	改进成本超过了预知的收益
根本原因	<ul style="list-style-type: none"> ● 倾向于只专注控制和性能的改进，而不是改进与创新的效率 ● 改进方案不适当的阶段和改进收益和成本之间明确关系的预防措施 ● 优先处理的是复杂、昂贵的解决方案而不是低成本的、容易的解决方案

	<ul style="list-style-type: none"> ● 重要的 IT 预算和人力资源都已致力于维护现有的基础设施，而留给 GEIT 处理的是有限的目标资金和人员时间
成功因素	<ul style="list-style-type: none"> ● 确定基础设施、流程和人力的范围，如标准化、较高的成熟度水平和较少的事件，在哪可以通过更好的治理产生效率和直接的成本节约 ● 优先处理基于效益和实施的简单，尤其是速效方案
问题	IT 和企业之间缺乏信任和良好的关系
根本原因	<ul style="list-style-type: none"> ● 遗留问题在于缺少项目和服务交付的 IT 痕迹记录 ● 缺乏业务问题和价值高低的 IT 理解 ● 范围和期望值没有正确阐述和管理 ● 在业务中不清晰的治理角色、责任和职责，造成退位的关键决策 ● 缺乏支持信息和需要改进的度量体系说明 ● 不愿错误被证明，普遍抵制变革
成功因素	<ul style="list-style-type: none"> ● 促进开放和透明的绩效沟通与公司的绩效管理相联结 ● 关注业务层面和服务能力 ● 发布实际的结果和经验教训有助于建立和维持信誉 ● 确保 CIO 在建立信任和关系上发挥了有效的作用和领导作用 ● 规范化业务治理中的角色和责任制，以便制定的职责是清晰的 ● 确认和沟通表明真正的问题，需要避免的风险和获得的收益(在业务项目)关系到提出的改进 ● 关注变革启动方案

阶段 4—我们需要做什么？

图 11 列出了在阶段 4 中的问题和根本原因及成功因素。

图 11—阶段 4：我们需要做什么？	
问题	未能了解环境
根本原因	<ul style="list-style-type: none"> ● 没有足够考虑变革文化，利益相关者认知和组织的变革要求 ● 没有足够考虑在 IT 与宽泛企业之间已有的治理实力和实践
成功因素	<ul style="list-style-type: none"> ● 完成利益相关者评估和关注变更启动方案的开发 ● 在 IT 与宽泛企业之间建立和利用现有的优势和良好的做法。避免只为 IT “重建轮回” ● 了解不同的支持群体，他们的目标和思维模式
问题	不同程度的复杂性(技术上、组织上和运营模式上)
根本原因	<ul style="list-style-type: none"> ● 缺少对 GEIT 实践的了解 ● 试图马上实施很多内容 ● 优先考虑关键的和难以改进的而没有一点实践经验 ● 复杂的或多运营模式
成功因素	<ul style="list-style-type: none"> ● 教育和培训 COBIT5 和实施方法 ● 分解为较小的项目，每次建立一个步骤，优先考虑速效方案 ● 从不同的支持群体收集改进需要，关联和优先考虑他们，而且对照到变革启动方案 ● 关注实施阶段的业务优先顺序
问题	难于理解 COBIT5 和相关框架，过程和实践

根本原因	<ul style="list-style-type: none"> ● 不足的技能 and 知识 ● 照搬最佳实践，不适合他们 ● 只关注过程，不关注其它促成因素，如角色和职责及应用技能
成功因素	<ul style="list-style-type: none"> ● 教育和培训 COBIT5，其它的相关标准和最佳实践及实施方法 ● 如果需要，取得能够胜任的和有经验的外部指导和支持 ● 适应和调整最佳实践以适合企业环境 ● 在设计过程考虑和应对技能、角色和职责、流程所有权、目的和目标、和其它促成因素的要求
问题	抵制变革
根本原因	<p>抵制是一种自然的行为反应，当维持现行状态受到威胁时，但它也表明了一个基本内容，如：</p> <ul style="list-style-type: none"> ● 对什么是需要的和为什么它是有用的误解 ● 预知工作量和成本会增加 ● 不愿意承认短处 ● 没有创新的综合症状，基础是通过迫使通用的治理框架运用到企业 ● 根深蒂固的思维/威胁作用或权力基础
成功因素	<ul style="list-style-type: none"> ● 关注具体核心问题和驱动的沟通意识 ● 通过企业和 IT 管理和利益相关者的培训提高意识 ● 使用有经验的变革推动业务和 IT 技能 ● 跟踪常规的重要阶段以确保参与各方实现了实施收益 ● 选择速效方案和较易获得的成果作为提供价值的开放式工具 ● 采用通用的框架如 COBIT5 关系到企业环境 ● 关注变革启动方案如： <ul style="list-style-type: none"> -开发 -培训 -指导 -咨询 -技能传输 ● 举办方法演示，发现领先者以促进收益

图 11—阶段 4：我们需要做什么？（续）

问题	未能采取改进
根本原因	<ul style="list-style-type: none"> ● 外部专家独立设计解决方案，或宏伟的解决方案没有适当的解释说明 ● 内部 GEIT 团队独立运营而且非正式的代替了真正的流程所有者，造成误解和抵制变革 ● 关键利益相关者的不恰当支持和指导，导致 GEIT 产生没有有效的所有权关系的新政策和程序
成功因素	<ul style="list-style-type: none"> ● 保证流程所有者和其它利益相关者在设计阶段参与 ● 使用向导及演示进行适当的培训而获得认同和支持 ● 开始速效方案，论证收益和从这构建 ● 寻找想要改进的支持者，而不是抵制的强制人 ● 促使管理结构分配角色和职责，致力于他们的持续运营，和监控合法性 ● 加强从外部专家到流程所有者的知识传递 ● 分派职责和授权流程所有者
问题	难于整合内部治理方法与外包伙伴的治理模式
根本原因	<ul style="list-style-type: none"> ● 担心暴露不适当的做法 ● 缺乏与外包供应商明确的和/或分享的 GEIT 需求 ● 不清晰的角色和职责分配 ● 方法上和期望值的差异

成功因素	<ul style="list-style-type: none"> ● 实施中涉及到的供应商/第三方和运营活动应适当 ● 合同中包含条件和审计权 ● 寻找结合框架和实施方法的方法 ● 事前处理角色、职责和治理结构及第三方，而不是事后 ● 根据（通过审计和检查记录）服务供应商流程，人和技术与 GEIT 实践和水平比较
------	--

阶段 5—我们怎样才能到达？

图 12 列出了在阶段 5 中的问题和根本原因及成功因素。

图 12—阶段 5：我们怎样才能到达？	
问题	缺乏实施保证的认识
根本原因	<ul style="list-style-type: none"> ● 过于乐观的目标，低估所需要的努力 ● IT 的补救方式和集中于运营问题 ● 缺少专用的资源或能力 ● 已分派的优先顺序错误 ● 范围与要求不一致或实施者的误解 ● 项目管理原则，如业务情况，没有很好地应用 ● 对业务环境的不充分领悟，如运营模式
成功因素	<ul style="list-style-type: none"> ● 期望值管理 ● 遵循的指导原则 ● 保持 IT 简单的、现实可行的和注重实效的 ● 把整个项目分解为小的可实现的项目，增进经验和效益 ● 确保实施范围基于要求和所有利益相关者对将交付什么都有相同的认知 ● 关注促成业务价值的实施 ● 确保专用资源的分配 ● 应用项目管理和治理原理 ● 利用现有的机制和工作方法 ● 确保对业务环境的充分领悟

图 12—阶段 5：我们怎样才能到达？（续）	
问题	试图一次做得太多，处理过于复杂或难度大的问题
根本原因	<ul style="list-style-type: none"> ● 缺少范围和投入量(如人员方面，建立通用的语言) ● 没有理解承受变革的能力(太多的其它行动) ● 缺少项目方案和管理，没有建立基础和到期的成果 ● 实施的过度压力 ● 没有启用速效方案 ● 重新构建推动力而没有利用原有内容作基础 ● 缺乏深入了解组织的前景 ● 缺乏技能
成功因素	<ul style="list-style-type: none"> ● 应用方案和项目管理原则 ● 运用重要里程碑

	<ul style="list-style-type: none"> ● 优先排序 80/20 任务(用 20%的投入量获得 80%的收益)且以正确的顺序来仔细地排序。启用速效方案 ● 建立信任/信心。以足够的技能和经验来保持 IT 的简单和实用 ● 重用原有内容作基础
问题	IT 和/或业务补救方式和/或没有很好的优先顺序和未能关注治理
根本原因	<ul style="list-style-type: none"> ● 缺乏资源或技能 ● 缺乏内部流程，内部效率低下 ● 缺乏强大的 IT 领导作用 ● 太多的解决方法
成功因素	<ul style="list-style-type: none"> ● 运用良好的领导技能 ● 获得高层的承诺和推动，这样组成的人员有效地关注 GEIT ● 在运营环境解决根本原因(外部的干预，管理 IT 的优先处理) ● 应用紧密的纪律处理/管理业务需求 ● 运用适当的外部资源 ● 获得外部协助
问题	缺乏所需的技能和能力，如了解治理、管理、业务、流程、软件技能
根本原因	<ul style="list-style-type: none"> ● 没有充分了解 COBIT 和 IT 管理最佳实践 ● 业务和管理技能常常不包括在培训中 ● IT 人员对非技术领域不感兴趣 ● 业务人员对 IT 不感兴趣
成功因素	<ul style="list-style-type: none"> ● 关注变革启动方案 <ul style="list-style-type: none"> -开发 -培训 -指导 -咨询 -反馈到录用流程 -交叉技术

阶段 6—我们到达了吗？

阶段 7-怎样保持推进的动力？

图 13 列出了在阶段 6 和阶段 7 中的问题和根本原因及成功因素。

图 13—阶段 6：我们到达了吗？阶段 7-怎样保持推进的动力？	
问题	未能采用或应用改进
根本原因	<ul style="list-style-type: none"> ● 解决方案太复杂或不切实际 ● 解决方案形成于独立的顾问或外部专家 ● 最佳实践照搬，而没有为适合企业运营进行量身定制 ● 解决方案不由流程所有者/团队“拥有” ● 组织缺乏明确的角色和职责 ● 管理者没有授权和支持变革 ● 抵制变革 ● 缺少了解怎样应用新的流程或开发工具 ● 技能和资历与角色要求不匹配

成功因素	<ul style="list-style-type: none"> ● 关注速效方案和管理项目 ● 做小的改进以检查方法和确信解决的问题 ● 在改进进展中包括流程所有者和其它利益相关者 ● 确信角色和职责是清晰和可接受的，是否需要变革角色和工作说明 ● 驱动改进来自于整个企业的管理 ● 需求的地方运用适当的培训 ● 试图自动化之前开发流程 ● 重组，如果需要，使用更好的流程所有权 ● 与个人能力和特点匹配角色（特别是那些成功实施的关键人员） ● 提供有效的教育和培训
问题	难于展示或证明收益
根本原因	<ul style="list-style-type: none"> ● 目标和衡量体系没建立或成果的有效性 ● 实施后没有使用效益跟踪 ● 减少收益的关注和价值的获得 ● 缺乏成功的有效沟通
成功因素	<ul style="list-style-type: none"> ● 设置清晰的、可衡量的、切实可行的目标(改进的预期效果) ● 设置实用的绩效指标(监控改进是否驱动了目标的实现) ● 平衡记分卡显示了正衡量的绩效是怎样的 ● 业务的有效沟通影响结果条件和获得的收益 ● 实施速效方案和在短时间范围内交付解决方案
问题	失去兴趣和动力
根本原因	<ul style="list-style-type: none"> ● 持续改进没有企业文化部分 ● 管理没有驱动可持续的结果 ● 资源集中于补救和服务交付，没有集中于改进 ● 人员没有积极性，不能看到采用和驱动变革带来的个人利益
成功因素	<ul style="list-style-type: none"> ● 确保管理层定期沟通和加强必要的有力的和可靠的服务、解决方案和良好的治理。实现成功改进的所有利益相关者的有效沟通 ● 再访利益相关者和得到他们的支持以“激发”推动力 ● 如果资源不足，抓住机会实施改进“在工作上”作为项目日常工作的部分 ● 关注常规的和可管理的改进任务 ● 获得外部协助，但保持参与 ● 调整个人奖励系统与流程和组织绩效改进目标和衡量体系相一致

六、促进变革

变革启动的必要性

成功实施或改进取决于以正确的方法实施了合适的变革(良好的实践)。在很多企业,把明显重要的放在第一方面,但在变革的人、行为、文化方面的管理和激励利益相关者支持变革不够重视。变革启动是 GEIT 实施的最大挑战之一。

它不应具有各种利益相关者参与,或受到影响,新的或修正的治理安排将必须立即接受和采用变革。不知和/或抵制变革需要通过结构化和积极的态度来处理的可能性。同样,方案的最佳认知度应是通过定义贯穿项目的不同阶段要沟通什么、以什么方式沟通和由谁沟通的沟通方案来实现的。

当在检查近期主要的 IT 改造活动时,US 事务部(VA)提到:VA 主要挑战将面对实现这次改革以获得所有 VA 人员的认可和支持,包括领导、中层管理人员和外地员工。VA 已表明如果只做技术改造,这种投入不可能成功。它认可了需要达到可接受的人的因素,变革企业和变革业务实施的方法都是成功的关键

在很多企业,在变革的人、行为、文化方面的管理和激励利益相关者支持变革没有足够重视。

COBIT5 定义了变革启动为:

准备和提交给所有利益相关者参与变革从当前状态到期望的将来状态的一个系统化的过程。

所有关键利益相关者应参与。在较高水平下,变革启动通常需要:

- 评估变革对企业、人员和其他利益相关者的影响
- 设立关于人力/行为方面和相关措施及说明的将来状态(愿景)
- 建立“变革响应计划”以前瞻性地管理变革影响和最大程度参与整个过程。这些计划尽可能包括培训、有效沟通、组织设计(工作内容、组织的结构)、流程重组和更新绩效管理系统
- 持续衡量变革过程走向期望的将来状态

根据典型的 GEIT 实施,变革启动的目标含有业务和 IT 领导为例的企业利益相关者和鼓励所有级别的员工根据期望的新方法工作。

例如期望的行为包括:

- 遵循约定的流程
- 参与定义 GEIT 结构如变革审批或顾问委员会
- 执行明确的指导原则、政策、标准、流程或实践如关于新的授权或安全的政策

这可能是最好的实现通过获得利益相关者的承诺(关注的程度和应有的关注,领导作用,和工作人员的有效沟通和响应)和获取的收益。必要地,需要加强合法性。也就是说,人、行为和文化障碍必须克服以便有共同利益对可能采用的,逐步灌输将采用和确保有能力采用新的方法。这可能是有用的凭借企业内部之间或必要的外部顾问促进行为变革的变革启动技术。

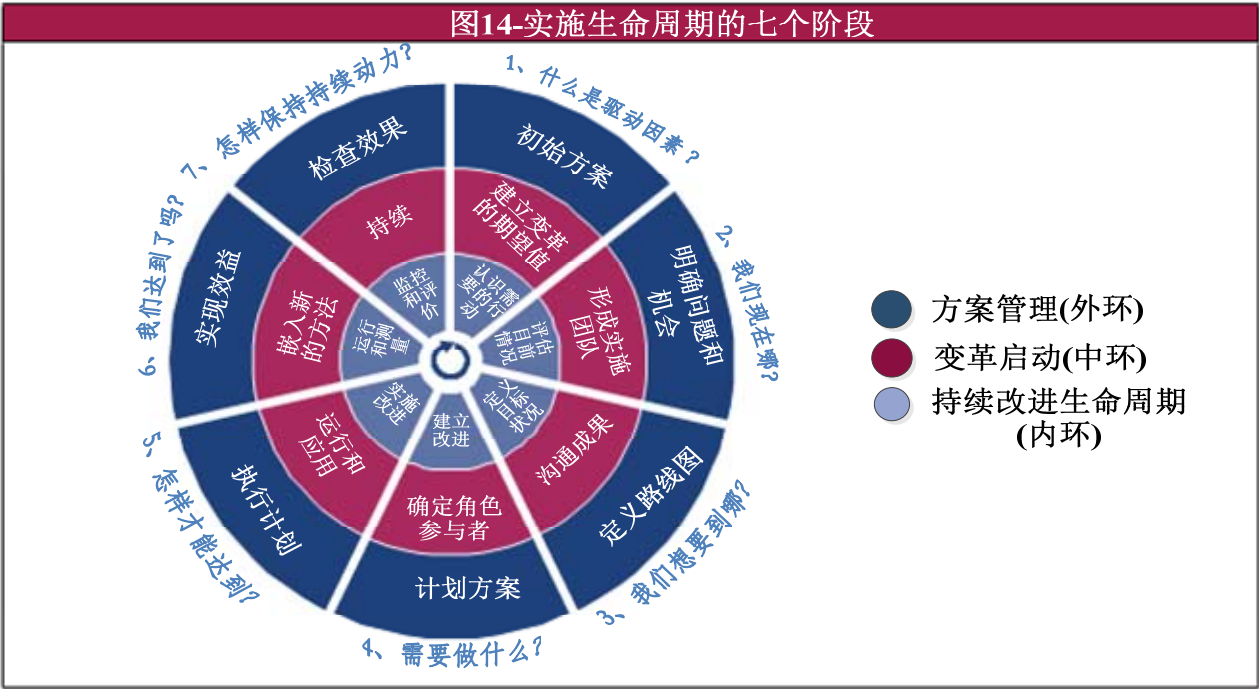
GEIT 实施的变革启动

人、行为和文化障碍必须克服以便有共同利益对可能采用的，逐步灌输将采用和确保有能力采用新的方法。

- 启动变革多年来已明确各种方法而他们提供的宝贵投入能够被使用于实施生命周期。启动变革最广泛接受的方法之一是由 John Kotter 开发的：
1. 建立紧迫感使命
 2. 形成强大的指导联盟
 3. 创建一个简洁表达的明确愿景
 4. 有效沟通愿景
 5. 授权其他人遵照愿景行动
 6. 计划和创建短期赢利
 7. 加强改进和产生更多的变革
 8. 使新的方法制度化

选择的 Kotter 方法作为范例且适用于 GEIT 实施的具体要求或环境。在图 14 中图解了变革启动的生命周期。

以下部分建立了一个高级别，而不是全部，简略地概述了变革启动生命周期的每个阶段，适用于典型的 GEIT 实施。



在变革启动生命周期创建适当环境的阶段

应分析整个企业环境以确定最恰当的变革启动方法。这将包括如管理方式，文化(工作方法)，正式和非正式关系和态度等方面。了解其它的 IT 和企业开展的新计划和措施也是很重要的，以确保考虑了相互关系和影响。

从一开始就应确保变革启动所需的技术、能力和可应用和使用的经验，如，通过从 HR 的职责或通过外部协助获得包含的资源。

作为这个阶段的成果，适当的平衡指导性的和包含一切变革启动活动要求提供持续的收益的计划性。

阶段 1：建立变革的愿望

这一阶段的目的是了解预想变革的广度和深度，受影响的不同利益相关者，影响的本质和来自每个利益相关集团的参与要求，以及当前的准备和适应能力。

当前的核心问题和触发事件可以为建立变革的愿望提供一个良好的基础。”提醒服务”，方案的最初沟通，可能与企业正经历的工作问题相关。当然，最初的收益也与企业高度可见的领域连接，为进一步变革和更广泛的承诺和支持创建一个平台。

而有效沟通是贯穿于实施或改进计划的普遍思路，最初的沟通或提醒服务是最重要之一且会表现出高级管理层的承诺。因此，理论上应是执行委员会和首席执行官(CEO)的有效沟通。

阶段 2：形成一个有效的实施团队

在聚集有效的实施团队中考虑的方面包括涉及业务和 IT 的适当领域以及知识和专业技术，经验，信誉，和权威的团队成员。获得一个独立、客观的观点，由外部各方提供如顾问和变革代理商，也是非常有益通过帮助实施过程或解决企业内部现有的技能差距。因此，要考虑的其它方面是适当地组合内外部资源。

团队的实质将会保证到：

- 一个明确的成功愿景和雄伟的目标
 - 在所有的团队成员，所有的时间使用最好的
 - 团队流程、职责和沟通的清晰度和透明度
 - 完善的、相互的支持和相互成功的保证
 - 彼此的职责和共同的责任
 - 自身绩效和作为团队表现方式的持续衡量
 - 在舒适环境外的生活，总是寻找改善的方法，发现新的可以利用和改善的余地和包括变革
- 这是很重要的在企业的不同地区确认可能的变革代理商以便核心团队从事于支持愿景和级联变革。

阶段 3：有效沟通期望的愿景

一个高层次的变革启动计划应与整体项目计划相连接制订。变革启动计划的关键要素是战略沟通，将提出核心拥护者团队是谁，他们的行为规范和信息要求，沟通渠道和原则。

实施或改进方案的期望愿景应是那些受此影响的语言上的沟通。有效沟通应包括理由和变革的收益以及没有开始变革(目的)的影响，愿景(图片)，实现愿景(计划)的路线图和要求不同利益相关者(部分)参与。高级管理层应传递关键的消息(如期望的愿景)。在沟通中应注意行为/文化和提到的合理方面，重点在于双方的沟通。反应、建议和其它反馈将会遵此行动或获取。

阶段 4：授权任务参与者和确认速效方案

设计和构建核心的改进，制定变革响应计划是为了授权各种不同的任务参与者。这些范围会包括：

- 组织的计划变革如工作内容或团队结构

- 组织的变革如流程变动或物流
- 人员管理变革如需要培训和/或绩效管理和薪酬系统的改变

任何可实现的速效方案对于变革启动远景都是很重要的。这些与第三章讨论过的核心问题和触发事件相关。可见的和明确的速效方案可以为方案建立动力和信誉，有助于解决可能存在的任何疑问。

在设计和构建核心的改进中使用的参与方式是急需的。通过那些受变革影响在实际设计中的参与，如研讨会和汇报会议，会增加支持。

阶段 5：促进运营和使用

作为核心实施生命周期的实施行动，变革响应计划也是要实施的。

以已实现的速效方案作为基础，而提出行为和文化方面更为广泛的变革。(如涉及担心责任缺失，新的期望值和未知任务的问题)

平衡团体和个人的参与这是很重要的以增加支持和保证及确保所有的利益相关者都获得了变革的全部视角。

解决方案将会推出，而在这过程中，指导和引导非常的关键以确保领会了用户了用户环境。在行动的开始就已设立的变革必要条件和目标将会再访以确保它们都得到了适当处理。

成功的措施应确定且应包括难度大的业务措施和追踪人们对变革感受如何的认知措施。

阶段 6：嵌入新的方法

变革是持续的通过利益相关者的作用，如有意识的加强和持续的交流活动

作为已实现的具体成果，工作的新方法将成为企业文化的一部分且根植于它的规范和价值观(我们围绕这做事的方式)，如：实施政策、标准和程序。这变革实施应可被追踪，应评估变革响应计划的有效性和采取纠正措施的适当性。还应包括一直要求的执行的合规性。

沟通策略应保持持续不断的认识。

阶段 7：持续

变革是通过意识强化和不断的沟通活动来持续的，通过持续高级管理层的承诺来维持和论证。

七、实施生命周期的任务、角色和职责

实施生命周期的任务、角色和职责

实现 GEIT 的持续改进运用了实施生命周期的七个阶段。每个阶段描述为：

- 图表概括了阶段中每组任务参与者的职责。注意这些角色是通用的而不是每个角色必须存在于具体的职责中。

- 每个阶段的表包含：

- 阶段目标
- 阶段说明
- 持续改进的任务
- 变革启动任务
- 项目管理任务
- 适当要求的输入例子
- 提议使用 ISACA 和其它框架项目
- 需要产生输出

- RACI 图描述了来自持续改进(CI)的关键活动、变革启动(CE)和项目管理(PM)任务中谁执行、负责、商议和告知，与交叉参照相符合。包含在 RACI 图的活动是最重要的，如产生交付物的活动或输出到下一阶段，有转折点连接他们，或对于整体活动的成功是关键。并不是所有的活动都包括在内，以益于保持这一指南的简明扼要。

本指南并不是指定性的，而是通用性的阶段和任务计划可改建以适合具体的实施。

阶段 1-驱动因素是什么？

图 15、16、17 和 18 描述了阶段 1

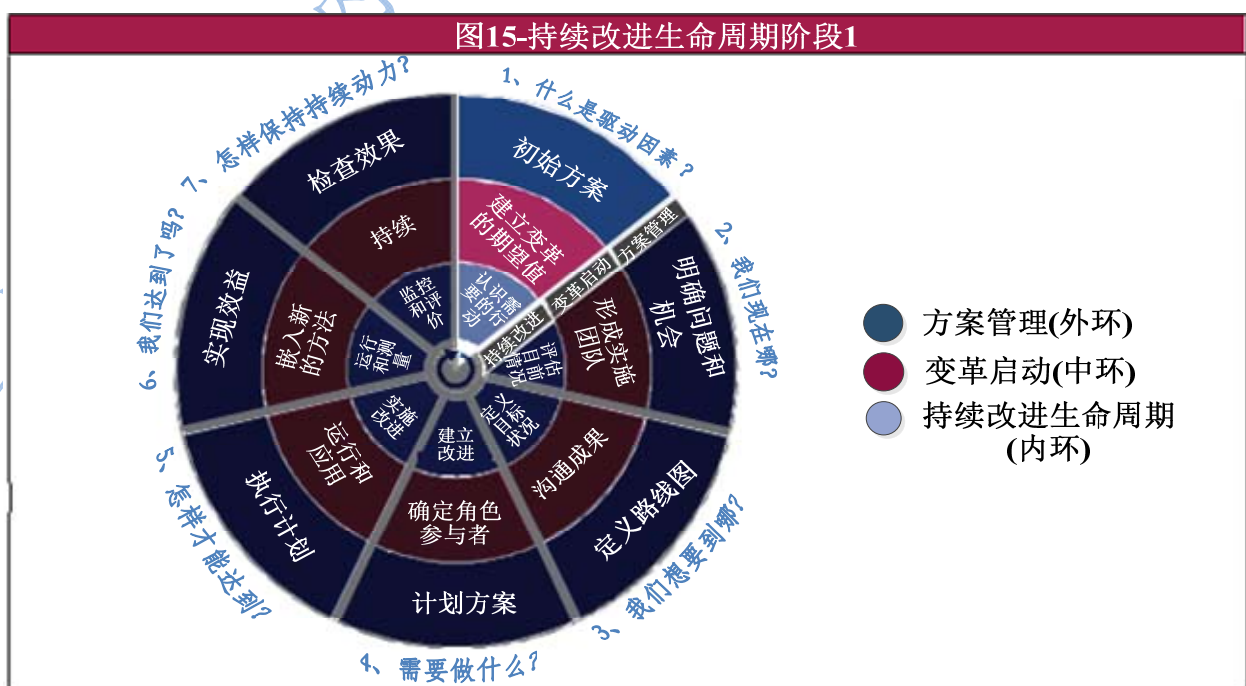


图 16—阶段 1 的角色

当你是.....	你在这的阶段是.....
董事会和执行委员会	提供涉及企业 IT 治理和管理中有关利益相关者的需要, 业务战略, 优先级、目标和指导原则的指导。批准高级别的方法。
业务管理者	与 IT 一起, 确保利益相关者的需要和业务目标已足够清晰地表达以有效促进业务目标转化为 IT 目标, 和为理解风险和优先排序提供输入信息。
IT 管理者	收集所有利益相关者的需求和目标, 获得对方法和范围的一致意见。提供专家建议和有关 IT 内容的指导。
内部审计	对所提议的活动和行动提供建议和质疑, 保证客观和均衡地做出决策。提供有关当前问题的输入信息。提供有关控制和风险管理实践和方法和建议。
风险、合规和合法	提供有关风险、合法和合规内容的建议和指导。保证所提议方法的管理满足风险、遵守和合规的要求。

图 17—阶段 1 描述

阶段 1	驱动因素是什么?
阶段目标	获得项目背景和目标 and 当前治理方法的了解。定义初始方案理念的业务模式。获得所有关键利益相关者的支持和承诺。
阶段描述	这阶段明确表达了在组织环境中采取行动的令人信服的理由。要定义这环境中的项目背景、目标和当前治理文化。定义初始方案的环境业务模式。获得所有关键利益相关者的支持和承诺。
持续改进任务(CI)	<p>认识到需要的行动:</p> <ol style="list-style-type: none"> 1. 确认当前治理的环境、业务 IT 和 IT 核心问题及症状触发所需的活动。 2. 确认业务和治理驱动和于改进 GEIT 和评估当前利益相关者需求的合规性要求。 3. 确认业务优先级和依靠 IT 的业务战略, 包括一切当前重要的项目。 4. 配合企业政策、战略、指导原则和一切进行的治理措施 5. 提高 IT 对企业和 GEIT 价值的重要性的执行意识 6. 定义 GEIT 政策、目标、指导原则和高级发展目标。 7. 确保执行委员会和董事会理解和批准高级别的方法及接受对重大问题不采取任何行动的风险。
项目管理 (PM) 任务	<p>发起项目:</p> <ol style="list-style-type: none"> 1. 提供 IT 执行战略委员会或等同(如果存在一个)同意的高层次的战略方向和设立高层次的项目目标。 2. 定义和分配项目间的高级别角色和职责, 从执行支持者到项目管理者 and 所有重要的利益相关者开始。 3. 制定一个概要的业务模式指明成功要素以用于有效的绩效监控和成功治理改进的报告。 4. 获得执行保证。
输入信息	<ul style="list-style-type: none"> ● 企业的政策、战略、治理和业务计划及审计报告 ● 其它与此可能相关和影响的主要的企业措施 ● IT 指导委员会绩效报告, 帮助台统计资料, IT 客户调查或其它能表明当前 IT 核心问题的输入信息 ● 任何有用的和相关的行业框架介绍, 案例研究和成功的经历, www.isaca.org/cobitcasestudies ● 具体的客户需求, 市场和服务战略, 市场定位, 企业愿景和宗旨表述。

图 17—阶段 1 描述（续）	
阶段 1	什么是驱动？
ISACA 的工具和其它框架	<ul style="list-style-type: none">● COBIT 5（企业目标，促成因素）● COBIT5: 启用的流程(EDM01; APO01; MEA01) , www.isaca.org/cobit● COBIT 5 实施(附录 A.映射到 COBIT 5 的主要问题, B.实例决策矩阵和 D.实例业务模式)● ISACA 相关产品如当前在 www.isaca.org 已确定的● 业务模式指南: 使用 Val IT 2.0
输出	<ul style="list-style-type: none">● 业务模式概要● 高级别角色和职责● 确定出的利益相关者图, 包括需要的支持和参与, 影响和作用, 和一致理解需要管理人力变化的投入量● 项目提醒服务(所有利益相关者)● 项目的强力沟通(关键利益相关者)

图 18 - 阶段 1 RACI 图									
主要活动	实施任务参与者职责								
	董事会	IT 执行委员会	CIO 首席信息官	业务执行经理	IT 经理	IT 所有者	IT 审计	风险和合规	项目指导
确认问题触发需要的行动(CI1)	C/I	A	R	R	C	C	C	C	R
确认业务优先级和 IT 战略影响(CI3)	C	A	R	R	C	C	C	C	R
得到管理层同意行动和获得执行保证(CI7)	C	A/R	R	C	I	I	I	I	R
逐步培养适当的紧急变革的能力(CE10)	I	A	R	R	C	C	C	C	R
产生令人信服的概要的业务模式(PM3)	I	A	R	C	C	C	C	C	R
RACI 图明确了谁是执行、负责、商议和/或告知									

阶段 2-我们现处于何位置？

图 19、20、21 和 22 描述了阶段 2

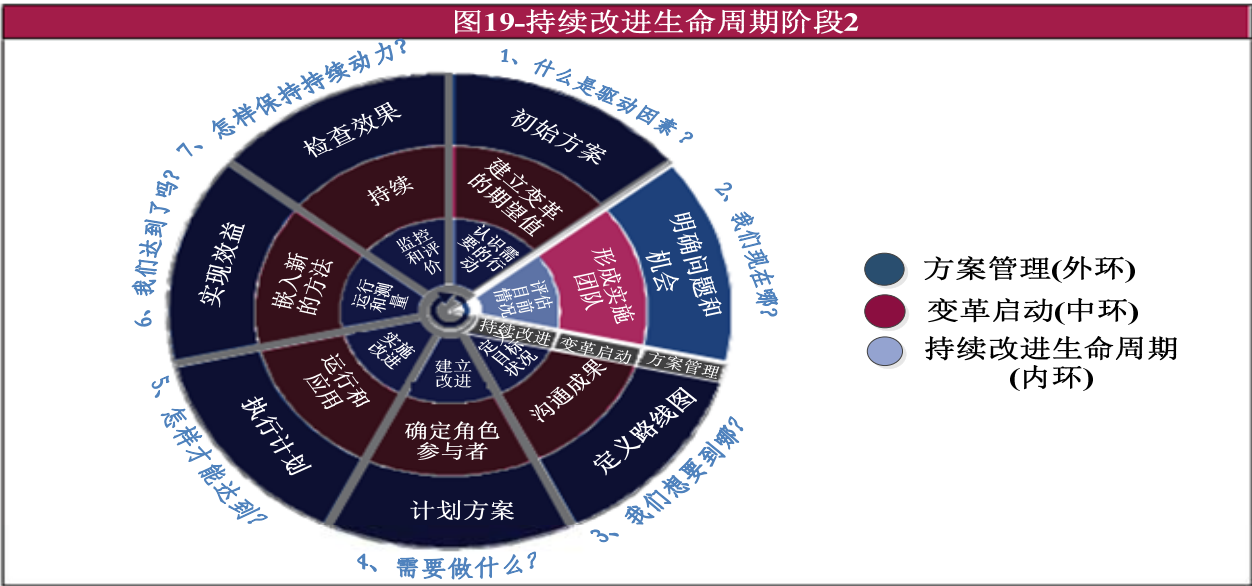


图 19—阶段 2 的角色	
当你是……	这阶段你的角色是……
董事会和执行委员会	验证和说明评估的结果/结论。
业务管理者	协助 IT 提供客户查看当前评估的合理性。
IT 管理者	确保公开、公平的评估 IT 活动。指导当前实践评估。取得一致意见。
内部审计	提供建议，提供输入信息和协助当前表达的评估。如果需要，独立地核实评估的结果。
风险、合规和合法	审查评估以保证风险、合规和合法问题已得到适当考虑。

图 20—阶段 2 描述	
阶段 2	我们现处于什么位置？
阶段目标	确保项目团队知道和理解企业的目标和怎样的业务和 IT 功能需要来自 IT 支持企业家目标交付的价值，包括当前的重大项目。确认关键的流程或在改进计划中提到的其它促成因素。为每一个选定的流程确认适当的管理实践。获得一个认识企业当前和未来对风险的看法和 IT 风险定位及确定它将会如何影响项目。确定已选定流程的当前能力。理解企业的能力和变革能力。
阶段描述	<p>这阶段确定企业和 IT 相关目标，如 IT 如何通过解决方案和服务促成已认可的企业目标。</p> <p>重点是确定和分析 IT 如何为企业创造价值，使企业转型为灵活的方式，使当前的业务流程更加有效，使企业更有影响力，而且满足企业治理相关的必要条件，如管理风险，确保安全且符合法律和法规要求。</p> <p>基于企业风险评测和它过去的风险及偏好，及实际效益/风险价值的实现，定义效益/风险价值的实现，方案/项目交付和服务交付/对企业和 IT 相关目标的 IT 运营风险。附录 C 包含一个表映射一般的风险情况对 COBIT 5 流程可用于支持这个分析。</p> <p>理解业务和治理驱动和风险评估用于侧重关键的流程以确保满足 IT 目标。这时，需要建立怎样成熟的、良好的管理和执行这些流程，基于流程描述，政策，标准，程序和技术规范以确定它们是否有可能支持业务和 IT 要求。这是通过评估每个流程的能力来实现的。</p> <p>在企业核心问题的存在可能会有助于哪一个是重要的 IT 流程的选择。这篇文档的附录 A 提供了普遍核心问题的实例映射(如在第四章讨论</p>

	的)对 COBIT 5 流程。流程参照模型内所有 37 个流程也有一个图表。
持续改进任务(CI)	<p>评估目前状态： 了解目前企业目标需要怎样的 IT 支持(COBIT 5 目标级联工具在 COBIT 5 框架和 COBIT 5 实施：促进流程提供的通用实例和可使用的相关关系)。</p> <ol style="list-style-type: none"> 1. 确认关键企业和支持的 IT 相关目标。 2. 建立 IT 分配的意义和本质（解决方案和服务）需要支持业务目标。 3. 识别关键治理问题和与当前和需要未来解决和服务有关的弱点，企业架构需要支持 IT 相关目标，和任何约束和限制。 4. 确认和选择关键流程以支持 IT 相关目标，如果合适，为每个选定的流程确定关键的管理实践。 5. 评估效益/风险价值的实现，方案/项目交付和服务交付/与关键 IT 流程有关的 IT 运营风险。 6. 确定和选择关键 IT 流程以保证风险可避免。 7. 了解管理所界定的风险可接受的定位。 <p>评估实际绩效（参考第七章，使用 COBIT 5 组件）</p> <ol style="list-style-type: none"> 8. 定义执行评估的方法 9. 记录理解当前流程如何实际解决早期选择的管理实践 10. 分析目前能力水平 11. 定义目前流程能力等级

图 21—阶段 2 描述(续)

阶段 2	我们现处于什么位置？
变革启动(CE)任务	<p>形成强大的实施团队：</p> <ol style="list-style-type: none"> 1. 从业务和 IT 召集具有适当知识、专业技能、经验、信誉和权威的核心团队以推动这次行动。确定最合适的人选(有效的领先者和利益相关者可信任的)领导这个团队。可以考虑外部各方，如顾问，作为团队的一部分提供一个独立、客观的观点或解决任何可能存在的技术差距。 2. 识别和管理可能存在于团队之间潜在的既定利益以建立必要程度的信任。 3. 为最佳团队创建适当的环境。这包括给予必要的时间和参与。 4. 在团队之间举行专题讨论会以建立共识(分享愿景)和为变革行动选择一个授权。 5. 确认变革代理商，核心团队可以与之使用级联支持的原则(具有不同层次级别支持愿景的支持者，广而告之速效方案，向下修改级联，可能存在的任何阻碍者和不信任者一起工作)以确保在生命周期的每个阶段期间广泛利益相关者的支持。 6. 确认在目前状态的评估的证明优势在于可以用于沟通的确定的因素以及可能会用于变革启动视角的潜在的速效方案。
项目管理(PM)任务	<p>确定问题和机遇：</p> <ol style="list-style-type: none"> 1. 检查和评价概要的业务模式，方案的可行性和可能的投资回报率(ROI)。 2. 分配角色、职责和流程所有者并确保受影响的利益相关者在方案的确定和执行的承诺和支持 3. 识别难题和成功因素
输入信息	<ul style="list-style-type: none"> ● 概要的业务模式 ● 高水平的角色和职责 ● 认可的利益相关者图，包括需要的支持和参与，影响和作用，和准备就绪及实施的能力或变革的支持 ● 项目提醒服务(所有利益相关者) ● 项目的强力沟通(关键利益相关者) ● 业务和 IT 计划和战略

	<ul style="list-style-type: none"> IT 流程描述、政策、标准、程序、技术规范 业务和 IT 作用的理解 审计报告、风险管理政策、IT 绩效报告/图表/记分卡 业务持续计划(BCPs), 影响分析, 合规要求, 企业架构, 服务级别协议(SLAs), 运营水平协议(OLAs) 投资项目和项目组合, 方案和项目计划, 项目管理方法, 项目报告
ISACA 资源	<ul style="list-style-type: none"> COBIT 5(企业目标—IT 相关目标级联和利益相关者需要目标的映射), www.isaca.org/cobit COBIT 5: 启用的流程 APO01; APO02; APO05; APO12; BAI01; MEA01; MEA02; MEA03(用于流程选择以及实施和方案计划) COBIT 5 实施(第五章.启动变革和附录 E. COBIT 4.1 能力属性表) COBIT 5 自评估指南(计划发布) ISACA 配套产品如当前在 www.isaca.org 已确定的
输出	<ul style="list-style-type: none"> 达成一致的 IT 和受 IT 影响的企业目标 达成一致的理解风险和导致不一致 IT 相关目标和服务及项目交付失败的影响。 选定的流程和目标 选定流程的目前能力级别 风险接受情况和风险简介 效益/风险价值的实现, 方案/项目交付和服务交付/IT 运营风险评估 建立的优势 在企业的不同地区和不同水平的变革代理商 核心团队和分配的角色和职责 评价的概要的业务模式 达成一致的理解问题和难题(包括流程能力级别)

图 22- 阶段 2 RACI 图

关键的活动:	实施任务参与者职责								
	董事会	IT 执行委员会	CIO 首席信息官	业务执行经理	IT 经理	IT 流程所有者	IT 审计	风险和合规	项目指导
确认支持业务目标的关键的 IT 目标(CI1).	I	C	R	C	R	C	C	C	A
确认支持 IT 和业务关键流程(CI4).		I	R	C	R	C	C	C	A
评估实现目标的相关风险(CI5).		I	R	C	R	R	C	R	A
确认关键的流程以确保关键的风险可避免(CI6)		I	R	R	R	C	C	R	A
评估关键流程的目前性能(CI1 到 CI11)		I	R	C	R	R	C	C	A
召集来自业务和 IT 的核心团队(CE1)		I	R	R	C	C	C	C	A
检查和评价业务模式(PM1)	I	A	R	R	C	C	C	C	R

RACI 图表明确了谁是执行、负责、商议和/告知

阶段 3-我们想要到达哪儿?

图 23、24、25 和 26 描述了阶段 3

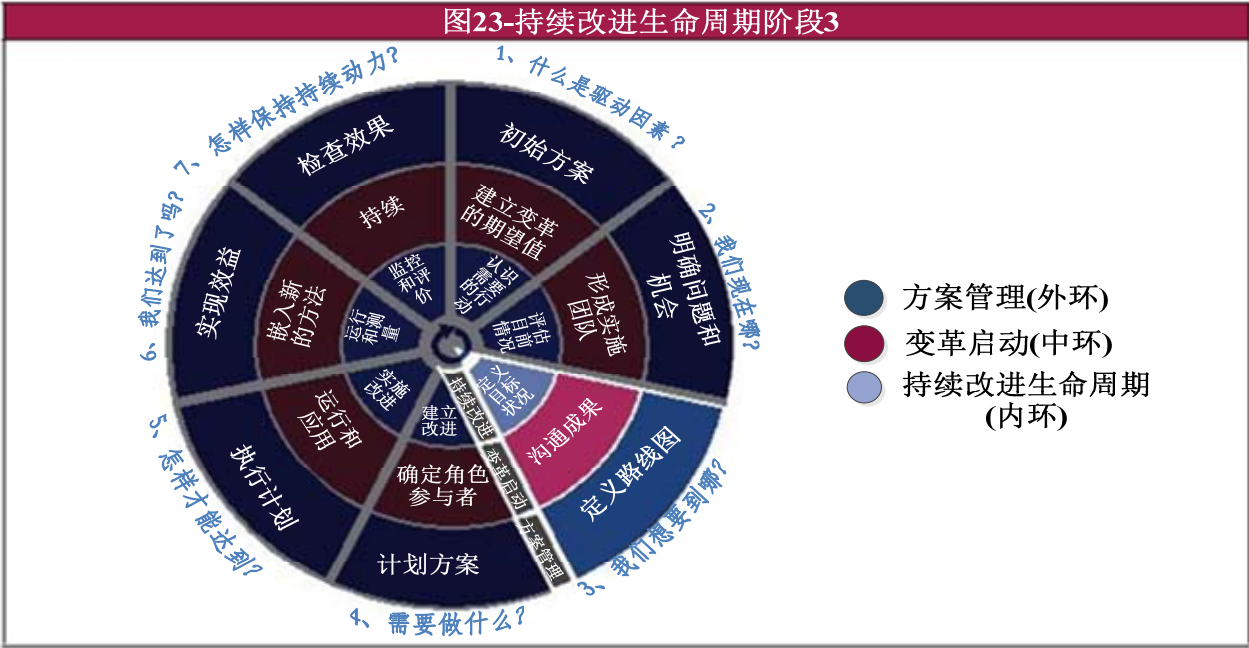


图 24—阶段 3 的角色	
当你是.....	这阶段你的角色是.....
董事会和执行委员会	设立优先等级，时间规模和预期有关的 IT 未来需要能力要求。
业务管理者	协助 IT 设立能力目标。确保预设的解决方案与企业目标保持一致。
IT 管理者	应用专业判断正式的改进优先计划和行动。获得与要求能力目标的共识。确保预设的解决方案与 IT 相关目标保持一致。
内部审计	提供建议和协助目标状态定位和差距优先。如果需要，独立地核实评估结果。
风险、合规和合法	检查计划以确保风险、合规和合法问题已适当提到。

图 25—阶段 3 描述	
阶段 3	我们想要到达哪儿？
阶段目标	确定每个已选定流程的目标能力。确定已选定流程的现在样子和即将达到的状况之间的差距，而把这些差距转换为改进的机遇。用此信息创建详细的业务模式和高级方案计划。
阶段描述	<p>基于评估目前状态流程能力级别，和利用企业目标到 IT 相关目标分析及识别早期完成流程的重要性结果，将会确定每个流程的恰当的目标能力级别。所选择的级别应考虑可用的外部和内部基准。这是很重要对于确保业务级别选择的适当性。</p> <p>在目前流程能力已确定和目标能力计划后，现在样子和即将达到的状态之间的差距应评价和识别改进的机遇。在差距已定义后，需要确定根本原因，普遍问题，剩余风险，现有优势和最佳实践以缩短这些差距。</p> <p>该阶段尽可能确定一些相对容易实现的改进，如加强培训，良好实践和标准化程序的分享；不过，差距分析可能需要相当多的在业务和 IT 管理技术到制定切实可行的解决方案的经验。保证行为和组织变革也需要经验。</p> <p>理解流程技术方法，先进的业务和技术专业知识，可能会需要业务知识和系统管理软件应用及服务。为确保该阶段有效的执行，团队与业务和 IT 流</p>

	程所有者及其它需要的利益相关者工作是很重要的。如果需要,还应该获得外部建议。应明确在缩短差距后将不会降低风险而通过管理正式接受。
持续改进(CI)任务	<p>定义目标状态和分析差距:</p> <ol style="list-style-type: none"> 定义改进的目标: <ul style="list-style-type: none"> 基于企业对性能和符合性的要求, 决定最初的思路每个流程的短期和长期目标能力级别。 在可能的范围内, 确定可采用的更好实践的内部的衡量标准。 在可能的范围内, 外部的基准与竞争对手和同行有助于决定目标级别选择的适当性。 做个目标级别合理性的“完整性检查”(单独的和全部的), 寻找实现什么和可值得拥有什么及在时间框架选择上可以产生最大的实际的影响。 分析差距: <ul style="list-style-type: none"> 运用目前能力的了解(通过属性)而比较它与目标能力级别。 利用现有优势, 尽可能处理差距, 查看指南来自 COBIT 5 管理实践和活 动及其它具体良好实践和标准, 如 ITIL, ISO/IEC 27000, TOGAF 和项目 管理知识体系(PMBOK)以缩短其它差距。 查找表明根本原因得到解决的模式。 识别潜在的改进: <ul style="list-style-type: none"> 按潜在的改进整理差距 确认未减轻的剩余风险和确保正式接受
变革启动(CE)任务	<p>描述和沟通期望的结果:</p> <ol style="list-style-type: none"> 描述高层次变革启动计划和目标, 其中将包括以下任务和组件。 制定沟通战略(包括核心群体, 行为规范和每个团体的信息要求, 核心消息, 最佳的沟通渠道及沟通原则)以优化意识和支持。 安全参与的意愿(变革的图片) 清楚地表达基本理由, 效益, 支持愿景的变革和描述不采取变革的影响(变革的目的) 在沟通和演示变革会如何实现收益中链接到行动的目标 描述实现愿景的高级别路径(变革计划)以及要求不同的利益相关者参与 者(变革间的角色) 让高级管理人员传递关键消息以“头部定调” 除了正式沟通外, 利用变革代理商的非正式沟通 通过行动沟通—指导团队以身作则 迎合他们的情感, 要求人们改变行为的地方 收集行动沟通反馈(反应和建议)和依此采用的沟通策略

图 25—阶段 3 描述 (续)

阶段 3	我们想要到达哪儿?
项目管理(PM) 任务	<p>定义路径图:</p> <ol style="list-style-type: none"> 设立高层次的项目方向, 范围, 收益和目标 确保与业务和 IT 战略相一致的目标 考虑风险和相应地调整范围 考虑变革启动含义 获得必要的预算和定义项目责任和职责 创建和评价详细的业务模式, 预算, 时间线和高级别项目计划。
输入信息	<ul style="list-style-type: none"> 达成一致的企业目标和对 IT 相关目标的影响 已选定流程的目前的能力级别 定义 IT 相关目标 选定的流程和目标 风险接受状况和风险介绍 评估效益/风险价值的实现, 方案/项目交付和服务交付/IT 运营风险评估

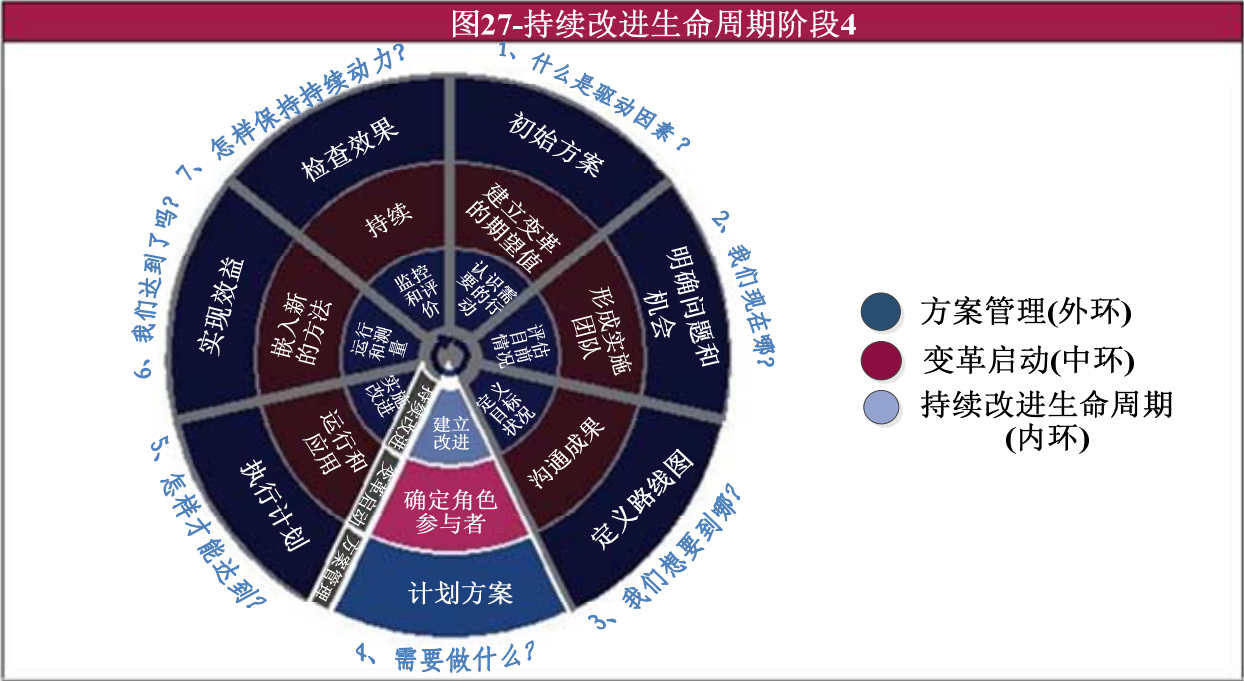


图 28—阶段 4 的角色	
当你是……	这阶段你的角色是……
董事会和执行委员会	考虑和对提议提出异议，支持合理的行动，提供预算和设定适当的优先级。
业务管理者	与 IT 一起，确保所提议的改进活动与达成一致的企业和 IT 相关目标保持一致和支持任何需要业务输入信息的活动或行动。保证需要的业务资源得以分配和可用。与 IT 取得一致的改进项目结果的测量标准体系。
IT 管理者	确保方案计划的可行性和合理性。确保计划是可实现的和执行计划有可用的资源。考虑计划和企业 IT 有效投资的投资组合的优先级以决定投资资金的基础。
内部审计	对确认的问题是有效的，业务模式是客观的且准确的描述，及计划是可实现的提供独立的保证。提供专家咨询和适当的指导
风险、合规和合法	确保任何识别的风险、合规和合法问题正进行处理，而且提议符合任何相关的政策、法规。

图 29—阶段 4 描述	
阶段 4	我们需要做什么？
阶段目标	把改进机遇转换为合理的促成项目。优先顺序和重点在高影响力项目。整合改进项目到整体方案计划中。执行速效方案。
阶段描述	<p>当所有潜在的改进活动已经确定时，这些活动应优先成为正式和合理的项目。具有高收益和相对容易实施的的项目应首先选择而且转换为正式和合理的项目，每一个项目计划包括项目促成到方案目标。这是很重要的检查目标是否仍然符合最初价值和风险的驱动。方案中更新的业务模式将会包括在项目中。任何未经批准的改进项目方案的详细资料应记录在登记簿，为潜在在未来考虑和机遇存在 而重新评估和支持，而且在适当时候，在稍后日期重新提交建议。</p> <p>基于时机表格，项目定义，资源计划和 IT 预算，确认的和优先处理的改进，现在变成了一组记录的项目以支持的整体改进方案。影响企业的已确定的执行方案和已筹划的变革计划描述了将确保的方案活动，实际上，通过项目交付的改进将会以可持续的方式推进企业。在这阶段一个重要的</p>

	<p>因素是测量标准的定义-如项目的成功衡量标准—将衡量流程改进是否有可能交付最初的业务收益。完整的改进方案计划表应记录在甘特图。</p> <p>新的项目会识别需要的变革或改进组织的结构或其它促使需求以保持有效的治理。如果需要，它可能是必要包括改善环境的行动(如第五章节描述的)。</p>
--	--

图 29—阶段 4 描述(续)

阶段 4	我们需要做什么？
持续改进(CI)任务	<p>设计和建立改进：</p> <ol style="list-style-type: none"> 1. 为每个改进，考虑可能的收益和易于的实施(成本、人工投入量、持续性)。 2. 为改进设立时机表格以识别优先考虑的行动(基于收益和易于的实施)。 3. 重点在选择显示高收益/高易于实施) 4. 考虑任何其它的行动显示高收益/低易于实施可能缩小范围的改进(分解为较小的改进和重新审视收益和易于实施) 5. 优先级排序和选择改进 6. 分析选定的改进的详细要求，高水平项目定义，考虑的方法，可交付的成果，资源需求，估算成本，估算时间规模，依赖关系和项目风险。运用可用的最佳实践和标准以进一步完善具体的改进要求。与经理和团队负责人讨论流程领域。 7. 考虑可行性，链接回最初的价值和风险驱动，及决定项目包括批准的业务模式。 8. 在登记簿上记录未批准的项目和行动，为可能的未来考虑。
变革启动(CE)任务	<p>授权任务参与者和确定速效方案：</p> <ol style="list-style-type: none"> 1. 在设计整个机制中通过那些受变革影响的参与来获得支持，如研讨会或检查流程和给予他们接受检查结果的责任。 2. 设计变革响应计划以主动管理变革影响和最大限度地参与整个实施过程(可能包括组织上的变革，如工作内容或组织结构；人员管理上的变革，如培训；绩效管理系统；或激励/薪酬和奖励系统) 3. 确认速效方案，证明改进方案的理念。这些应是可见和明确的，建立的动机和提供主动强化的过程。 4. 在可能的地方，依靠阶段 2 确定的任何现有的优势实现速效方案。 5. 确认现有企业可利用流程的优势。例如，在业务其它领域现有的项目管理优势，产品开发(避免重新再造的影响，和尽可能调整与目前企业一致的方法)
项目管理(PM)任务	<p>制定方案计划：</p> <ol style="list-style-type: none"> 1. 组织可能的项目到整体方案中，在优先排序，考虑预期结果的贡献，资源需求和依赖关系。 2. 使用投资组合管理技术确保方案符合战略目标及 IT 平衡了开展的新计划和措施。 3. 确认 IT 和业务组织改进方案的影响和指出怎样保持改进的动力。 4. 形成变革计划文档，任何迁移、转化、测试、培训、流程或其它活动必须包括在方案内作为实施的部分。 5. 确定和达成一致的测量标准，在原有方案成功因素方面衡量改进方案的结果 6. 指导业务的配置和优先处理，IT 和审计资源需要实现方案和项目目标 7. 确定项目投资组合以便方案将交付的需求结果 8. 确定需求交付成果，考虑全部活动范围需要满足的目标 9. 如果需要，为具体的项目方案指定项目指导委员会 10. 建立项目计划和报告程序以监控进展
输入信息	<ul style="list-style-type: none"> ● 选定流程的目标成熟度级别 ● 改进机遇的描述 ● 风险响应记录 ● 变革启动计划和目标 ● 沟通策略和变革愿景涵盖个 Ps(图片、目的、计划、部分)的沟通 ● 详细的业务模式

	<ul style="list-style-type: none"> ● 可能的工作表、最佳实践和标准、外部评估、技术评价 ● 可能的表格、项目定义、项目投资组合计划、资源计划、IT 预算 ● 早期阶段确认的优势
ISACA 资源	<ul style="list-style-type: none"> ● COBIT 5(启用模型), www.isaca.org/cobit ● COBIT 5: 启用流程(AP05, APO12, BAI01; 目标和测量方法标准体系) ● ISACA 配套产品如当前在 www.isaca.org 已确定的
输出	<ul style="list-style-type: none"> ● 改进项目定义 ● 明确的变革响应计划 ● 确认的速效方案 ● 未批准项目的记录 ● 相关联的单独计划分配资源, 优先顺序和交付成果的方案计划 ● 项目计划和报告程序通过投入的资源, 如技能、投资 ● 成功的测量标准体系

图 30 - 阶段 4 RACI 图

关键的活动:	实施任务参与者职责								
	董事会	IT 执行委员会	CIO 首席信息官	业务执行经理	IT 所有者	IT 流程所有者	IT 审计	风险和合规	项目指导
优先级排序和选择改进 (CI5).		A	R	C	C	R	C	C	R
确定和调整项目(CI6 和 CI7).		I	R	C	R	R	C	C	A
设计变革响应计划(CE2).		I	R	R	C	C	C	C	A
确定速效方案和依靠现有优势(CE3)		I	C	C/I	R	R	C/I	C/I	A
制定有分配资源的方案计划和项目计划 (PM1 到 PM10)		A	C	C	R	C	I	I	R

RACI 图表明了谁是执行、负责、商议和告知

阶段 5-我们如何到达那里?

图 31、32、33 和 34 描述了阶段 5

图31-持续改进生命周期阶段5



图 32—阶段 5 的角色

当你是.....	这阶段你的角色是.....
董事会和执行委员会	监控实施和提供所需要的支持和指导。
业务管理者	召集业务所有者参与实施，特别是受影响的业务流程和需要用户/客户参与的 IT 流程。
IT 管理者	保证实施包括所活动需要的全部范围(如政策和流程变革，技术解决方案，组织上的变革，新的角色和职责，其它的促成因素)，而且它们是切实可行和可实现的及尽可能地采用和使用。确保流程所有者参与进来，支持新的方法和承认结果流程。解决问题和管理风险在实施期间遇到的。
内部审计	检查和提供实施期间的输入信息以避免失去促成因素的识别和特别是事实之后的关键控制。提供实施中控制方面的指导。如果需要，提供项目/实施风险检查服务，监控可能危及实施的风险和对方案和项目团队提供独立的反馈。
风险、合规和合法	提供如在实施期间风险、合规和合法方面需要的指导。

图 33—阶段 5 描述

阶段 5	我们如何到达那儿?
阶段目标	实施详细的改进项目，利用企业方案和项目管理能力、标准和实践。监控、衡量和报告项目进展。
阶段描述	<p>被认可的改进项目，包括需要的变革活动，是现在准备实施的，因此在方案中确定的解决方案现可获取或开发和实施到企业中。因此，项目变成正常发展生命周期的部分和应通过建立方案和项目管理方法进行管理。推出的解决方法应符合既定的项目定义和变革计划以便改进可持续。</p> <p>该阶段通常涉及所有生命周期阶段的最大的投入和最长消耗时间。这是建议，然而，其投入的大小和花费的总时间不会过多地确保它是易于管理和在合理的时间框架内交付收益。当它还是一个学习所有参与的经验时，首次少量重复是极其真实的。</p> <p>监控每个项目的绩效以确保实现的目标。利益相关者的定期报告反馈保证了进展的了解和跟踪。</p>
持续改进(CI)任务	<p>实施改进：</p> <ol style="list-style-type: none"> 1. 在必要时，制定和获取解决方案，包括活动需要的全部范围，如文化，道德，和行为；组织结构；原则和政策；流程；服务能力；技能和能力要求；和信息 2. 当使用最佳实践时，采用和适应可用的指导以适合企业政策和程序的方法 3. 在真实的活动环境检查解决方案的实用性和适应性 4. 推出解决方案，考虑任何现有的流程和迁移需求
变革启动(CE)任务	<p>促进运营和使用：</p> <ol style="list-style-type: none"> 1. 以契机和信誉为基础的可以通过速效方案创建，然后引进更广泛和更有挑战的变革观点 2. 有效沟通速效方案的成功和认可及奖励参与其中的那些 3. 实施变革响应计划 4. 保证任务参与者拥有技能、资源和知识更广泛的基础，还有支持和保证变革 5. 平衡团队和个人的介入以确保通过利益相关者获得变革的整体看法 6. 广泛传递计划中文化和行为方面(涉及责任/独立性/决策的授权丧失的可能性，新的期望值和未知的任务) 7. 沟通角色和职责的使用 8. 定义成功的措施，包括那些业务视角和预知措施 9. 设立适当的指导和辅导以确保领会和支持 10. 闭合循环以确保所有变革需求已处理 11. 监控变革启动的有效性和采取必要的纠正行动
项目管理(PM)任	<p>执行计划：</p> <ol style="list-style-type: none"> 1. 保证方案的执行是基于该项目方案最新的和整体的(业务和 IT)计划

务	2. 指导和监控方案中所有项目的贡献以确保预期结果的交付 3. 提供定期更新的报告给利益相关者以确保了解和跟踪进展情况 4. 记录和监控重大项目的风险和问题，而且同意补救行动 5. 批准每个主要方案阶段的行动和与所有利益相关者沟通它 6. 批准任何重大变革的方案和项目计划
输入信息	<ul style="list-style-type: none"> ● 改进项目定义 ● 确定的变革响应计划 ● 确认的速效方案 ● 未批准项目的记录 ● 具有分配资源、优先级和交付成果的方案计划 ● 项目计划和报告程序 ● 成功的测量标准体系 ● 项目定义，项目甘特图，变革响应计划，变革策略 ● 整合的方案和项目计划
ISACA 资源	<ul style="list-style-type: none"> ● COBIT 5：启用流程（如最佳实践输入信息和 BAI01）， www.isaca.org/cobit ● ISACA 配套产品如当前在 www.isaca.org 已确定的
输出	<ul style="list-style-type: none"> ● 实施改进 ● 实施变革响应计划 ● 实现速效方案和变革成功的能见度 ● 成功的有效沟通 ● 确定的和沟通的通常业务环境的角色和职责 ● 项目变革日志和问题/风险日志 ● 确定的业务和预知成功的措施 ● 效益跟踪到监控实现

图 34 - 阶段 5 RACI 图

实施任务参与者职责									
	董事会	IT 执行委员会	CIO 首席信息官	业务执行经理	IT 所有者	IT 流程	IT 审计	风险和合规	项目指导
关键的活动:									
在必要时，制定和获取解决方案(CI1).		A	C	C	R	R	C	C	R
采用和适应最佳实践(CI2).		I	R	C	R	R	C	C	A
检查和推出解决方案(CI3 和 CI4).		I	R	C	R	R	C	C	A
利用速效方案(CE1 和 CE2)		I	C	C/I	R	R	C/I	C/I	A
实施变革响应计划(CE3)	I	I	R	C	R	R	I	I	A
指导和监控方案内的项目(PM2)	I	A	C	C	R	C	I	I	R

RACI 图表明了谁是执行、负责、商议和/告知

阶段 6-我们到达那儿了吗？

图 35、36、37 和 38 描述了阶段 6

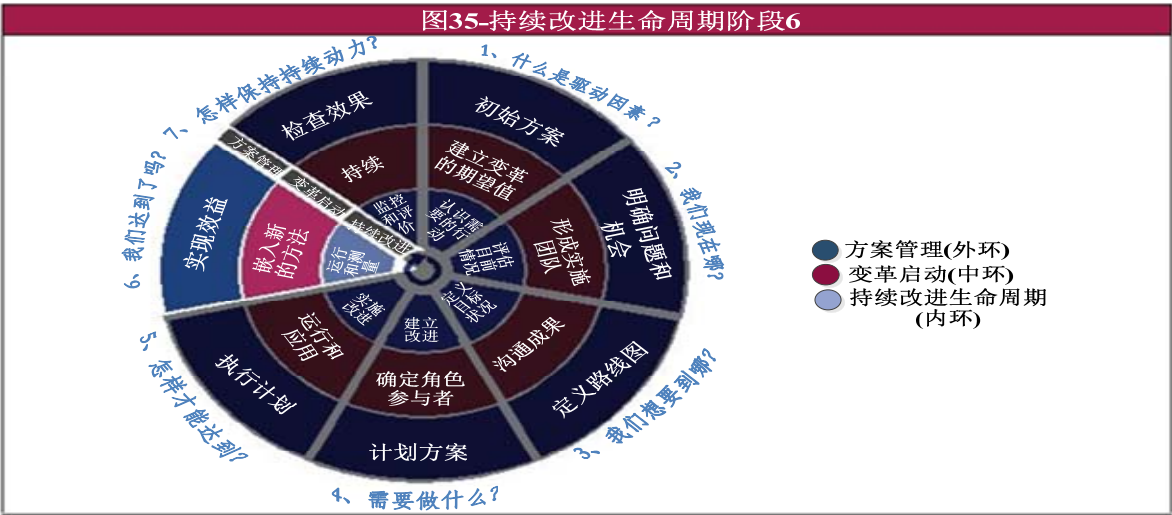


图 36—阶段 6 的角色	
当你是……	这阶段你的角色是……
董事会和执行委员会	评估满足最初的目标的绩效和确定实现预期的结果。考虑需要重定未来的活动和采取纠正行动。如果需要，协助解决重大的问题。
业务管理者	提供反馈和考虑开始新计划和措施的业务贡献的有效性。使用实际的结果改进目前业务相关活动。使用经验教训以适应和改进业务未来行动的方法。
IT 管理者	提供反馈和考虑开始新计划和措施的 IT 贡献的有效性。使用实际的结果改进目前 IT 相关活动。监控项目基于项目的关键性因为它们在进展中，使用方案管理和项目管理技术，及如果早期指明项目是偏离轨道且可能无法满足关键的重要阶段时，应准备改变计划和/或取消一个或多个项目或采取其它纠正行动。使用经验教训以适应和改进 IT 未来行动的方法。
内部审计	提供活动效率性和效果性的独立的评估。提供反馈和考虑开始新计划和措施的审计贡献的有效性。使用实际的结果改进目前审计相关活动。使用经验教训以适应和改进审计未来行动的方法。
风险、合规和合法	评估活动是否改进了企业确定的能力和管理风险和合法，监管和合约要求。提供反馈和作出任何必要的改进建议。

图 37—阶段 6 描述	
阶段 6	我们到达那儿了吗？
阶段目标	把项目绩效的测量标准体系和整体治理改进方案的收益实现融入定期和持续监控的绩效测量系统。
阶段描述	<p>通过 IT 相关目标和流程目标适宜技术的监控项目的改进描述是必要，如 IT 平衡记分卡(BSC)和证明变革结果已实现的收益记录。这将保证活动的继续跟踪依据最初企业和 IT 相关目标和持续交付预期业务收益。需要设立每个指标、目标，定期与实际值比较和使用绩效报告交流。</p> <p>为确保成功，绩效测量的肯定的和否定的结果都要报告给所有利益相关者这是至关重要的，将会建立可信度和能够及时采取纠正行动。项目应被监控因为它们在进展中，使用方案管理和项目管理技术，及如果早期指明一个项目是偏离轨道且可能无法满足关键的重要阶段时，应作出改变计划和/或取消项目的准备。</p>
持续改进(CI)任务	<p>执行和测量：</p> <ol style="list-style-type: none">1. 为每段商定的时间周期每个指标设置目标。目标应能促进 IT 绩效和改进监控活动及成功或可能失败的测定。2. 在可能时，对这些指标进行当前实际的测量。3. 采集实际的测量且定期与它们的目标相比较，如每月，基准和检查任何显著的差异。

启动(CE)任	<ol style="list-style-type: none"> 3. 监控是否分配了已出现的角色和职责 4. 跟踪变革和评估变革响应计划的有效性, 链接结果到初始变革的目的和目标。这应包括艰难的业务测量和认识能力的测量, 如认识能力调查, 反馈会议, 培训评估表。 5. 利用卓越的智囊提供灵感的来源。 6. 保持沟通策略实现持续意识和显著的成功 7. 确保所有任务参与者解决问题的内部沟通 8. 问题不能解决时, 升级到支持者 9. 在仍然需要时, 通过管理者授权执行变革 10. 为将来实施活动记录变革启动的经验教训
管理(PM)任	<p>实现收益:</p> <ol style="list-style-type: none"> 1. 监控方案违反业务模式目标的整体绩效 2. 监控投资绩效(成本违反预算和收益的实现) 3. 为随后的改进活动记录经验教训(肯定的和否定的)
信息	<ul style="list-style-type: none"> ● 实施改进 ● 实施变革响应计划 ● 实现速效方案和成功沟通 ● 明确和沟通业务运营环境的角色和职责 ● 项目变革日志和问题/风险日志 ● 明确业务和认识能力的成功测量 ● 因需求分析确认的 IT 目标和 IT 流程目标 ● 现有的测量方和/或记分卡 ● 业务模式收益 ● 变革响应计划和沟通策略
CA 资源	<ul style="list-style-type: none"> ● COBIT 5: 启用流程(如最佳实践输入和 EDM05, APO05, BAI01, MEA01) www.isaca.org/cobit ● ISACA 配套产品如当前在 www.isaca.org 已确定的
	<ul style="list-style-type: none"> ● 更新项目和方案记分卡 ● 变革有效性测量(业务和认识能力测量) ● 报告解释记分卡结果 ● 改进根深蒂固的运营 ● 关键指标增加到持续的 IT 绩效测量方法中

八

图 50 实施 RACI 图

关键的活动:	实施任务参与者职责								
	董事会	IT 执行委员会	CIO 首席信息官	业务执行经理	IT 经理	IT 流程所有者	IT 审计	风险和合规	项目指导
执行解决方案和获得绩效反馈 (CI1 到 CI3).		I	A	R	R	R	I	I	I
监控绩效违反成功的指标(CI4 和 CI5).		I	A	C	R	R	C	C	I
有效沟通肯定的和否定的结果(CI6).	I	I	A	C	R	C	I	I	I
监控所有者的角色和职责(CE3)		A	R	C	C	C	C	C	I
监控方案结果(实现的目标和实现的收益) (PM1 和 PM2)	I	A	C	C	C	C	C	C	R

RACI 图表明了谁是执行、负责、商议和/告知

阶段 7-怎样保持改进动力？

图 39、40、41 和 42 描述了阶段 7

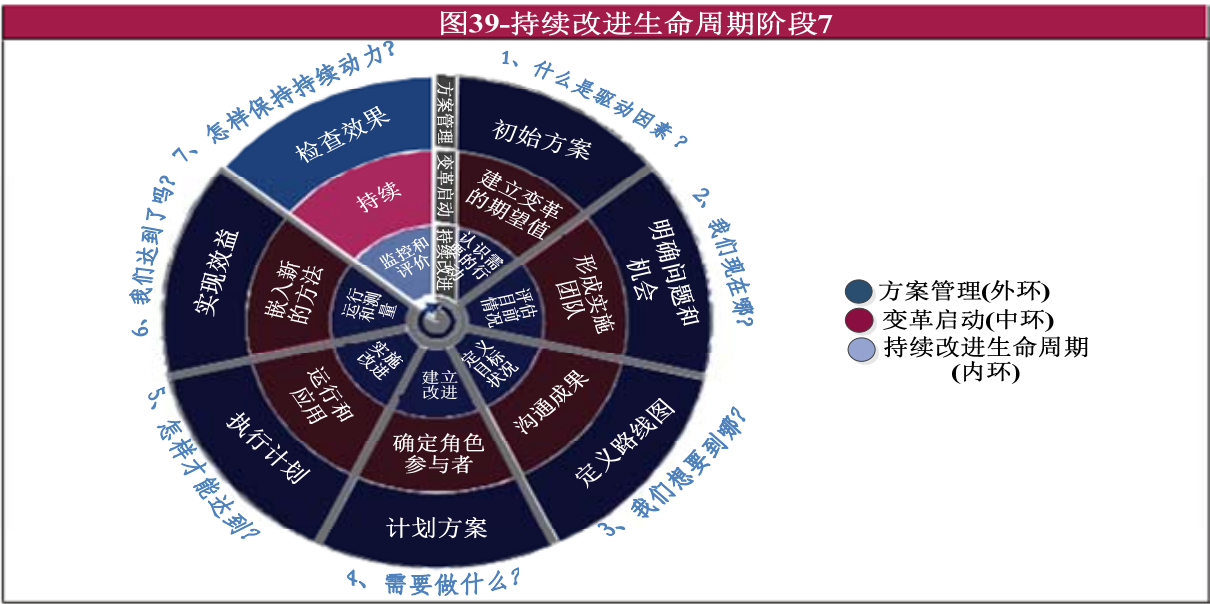


图 40—阶段 7 的角色	
当你是……	这阶段你的角色是……
董事会和执行委员会	提供指导，设定目标和为企业目前的方式，GEIT 改进分配角色和职责。延续“头部定调”，制定组织的结构，促进良好治理的企业文化和 IT 与业务之间及 IT 执行的问责制。保证 IT 的意识，新的业务目标和需求尽可能以及及时的方式适当的参与。
业务管理者	提供支持和承诺通过确实地与 IT 继续工作改进 GEIT 和使业务正常运营。验证新的 GEIT 目标与目前企业目标保持一致。
IT 管理者	驱动和提供强有力的领导作用保持改进方案的动力。作为正常业务实践部分参与治理活动。建立政策、标准和流程，确保治理适合业务正常运营
内部审计	提供目标和建设性的输入，支持自评，和提供管理治理有效开展的保证，由此建立 IT 的信心。提供基于整体治理方法运用 IT 共享的标准和业务基于 COBIT 框架的持续的审计。
风险、合规和合法	IT 的工作和业务预期的法律和法规要求，及确认和响应 IT 相关风险作为正常的 GEIT 的活动。

图 41—阶段 7 描述	
阶段 7	怎样保持改进动力？
阶段目标	评估结果和从项目获得的经验。记录和分享任何经验教训。改进组织结构，流程，变革企业行为的角色和职责以便 GEIT 适应业务正常运营且持续优化。确保新的需求活动驱动进一步的生命周期的重复。 持续的监控绩效，保证定期报告结果，和驱动责任和所有职责和责任的所有权。
阶段描述	该阶段促使团队确定是否按预期交付方案。可能会通过比较结果和原有的成功标准和收集团队的反馈及利益相关者的视角、研讨会和满意度调查来完成。经验教训可能包含团队成员和项目利益相关者运用于持续活动和改进项目的有用

	<p>价值信息。它涉及持续监控、定期传递报告，和问责制确定。</p> <p>确定进一步的改进和运用输入到生命周期的下一次迭代。</p> <p>在这阶段，企业应依靠治理实施项目的成功和经验教训建立和加强所有 IT 和业务利益相关者之间为持续 IT 治理改进的保证。</p> <p>政策、组织结构，角色和职责，和治理流程应制定和优化以便 GEIT 执行的有效性，作为正常业务实践，通过高级管理层表明，有这样的文化支持。</p>
持续改进(CI)任务	<p>监控和评价：</p> <ol style="list-style-type: none"> 1. 基于获得的经验，目前的业务目标为 IT 或其它触发事件确认新的治理目标和要求： <ol style="list-style-type: none"> a. 收集反馈和完成利益相关者满意度调查 b. 测量和报告实际的结果对最初建立成功的项目测量，和深入持续的监控和报告 c. 与项目团队成员和项目利益相关者完成促进项目的检查流程以记录和传递经验教训 d. 深入寻找高影响，低成本机遇以进一步改进 GEIT 2. 确认经验教训 3. 与利益相关者进一步沟通治理的要求和记录的运用作为输入到生命周期的下一次迭代
变革启动(CE)任务	<p>维持：</p> <ol style="list-style-type: none"> 1. 提供意识的增强和持续的沟通活动，以及表明持续高级管理层的承诺 2. 确定目标和需求的符合性 3. 持续监控变革自身，变革启动活动和利益相关者支持的有效性 4. 在需要时，实施纠正活动计划 5. 提供绩效反馈，奖励实现者和发布成功 6. 建立在经验教训上 7. 分享来自广泛企业开展新计划和措施的知识
项目管理(PM)任务	<p>检查项目的有效性：</p> <ol style="list-style-type: none"> 1. 在项目结束，保证项目检查开始和审核结论 2. 检查项目有效性
输入信息	<ul style="list-style-type: none"> ● 更新项目和方案记分卡 ● 变革有效性测量(业务和认识能力测量) ● 报告解释记分卡结果 ● 实施后检查报告 ● 绩效报告 ● 业务和 IT 战略 ● 新的触发如新的控制要求
ISACA 资源	<ul style="list-style-type: none"> ● COBIT 5: 启用流程(EDM01,APO01,BAI08,MEA01), www.isaca.org/cobit ● ISACA 配套产品如当前在 www.isaca.org 已确定的
输出	<ul style="list-style-type: none"> ● 建议进一步的 GEIT 活动 ● 利益相关者满意度调查 ● 记录成功事例和经验教训 ● 持续沟通计划 ● 完成奖励方案

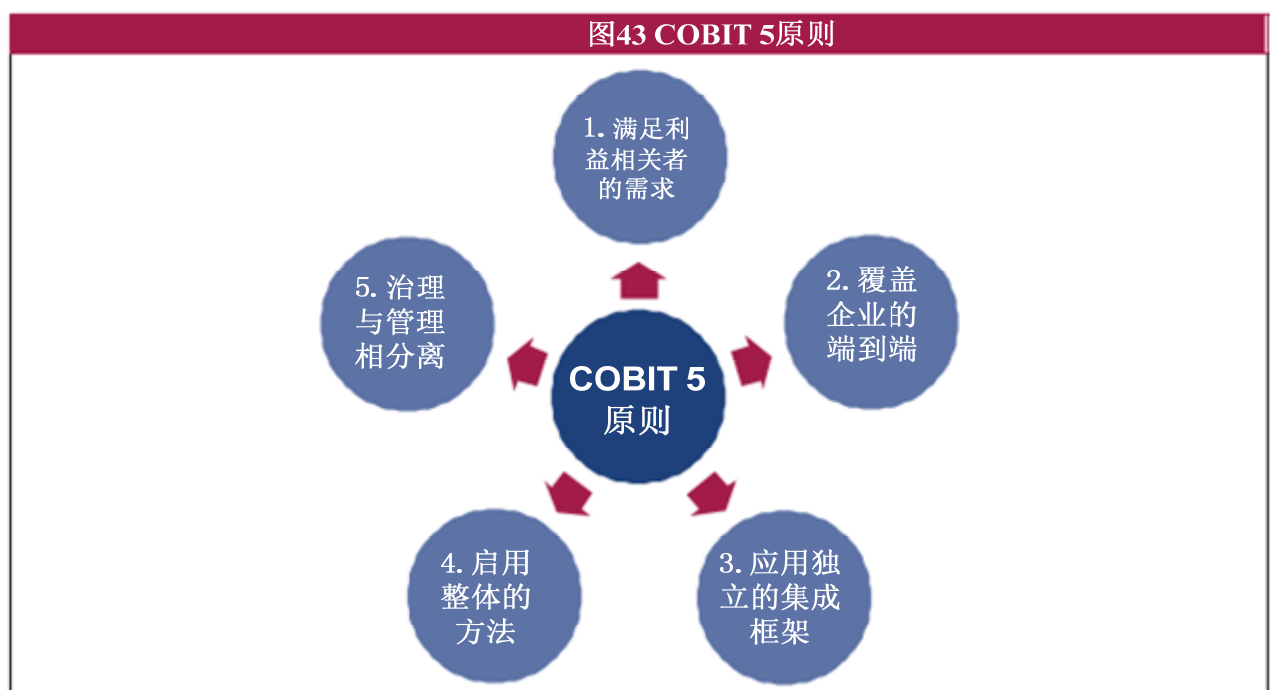
图 42- 阶段 7 RACI 图

实施任务参与者职责									
	董事会	IT 执行委员会	CIO 首席信息官	业务执行经理	IT 经理	IT 所有者	IT 审计	风险和合规	项目指导
关键的活动:									
确认新的治理目标(CI1)	C	A	R	R	C	C	C	C	I
识别经验教训(CI2)		I	A	C	R	R	C	C	I
维持和增强变革 (CE1)		A	R	R	R	R	C	C	I
确定目标和要求的符合性(CE2)	I	A	R	C	R	R	R	I	R
项目结束正式检查项目的有效性(PM1)	I	A	C	C	C	C	C	C	R
RACI 图表明了谁是执行、负责、商议和告知									

八、使用 COBIT5 组件

COBIT 4.1, Val IT and Risk IT 使用者的转换注意事项

COBIT4.1, VAL IT 和 RISK IT 已经用于 GEIT 实施活动的使用者可能会转换使用 COBIT 5 和受益于最新的和改进的指导, 它提供了企业改进生命周期的下一次迭代。COBIT 5 建立于先前的 COBIT, VAL IT 和 RISK IT 版本, 因此企业也会用早期的版本建立他们想要制定的内容。当采用最新的 COBIT 和其它的合适的指南时, 实施总会定制为适合具体企业的环境和要求。这些资料随着时间的推移因为条件变化和实践改善还会继续变化。图案 3 显示了 COBIT 5 原则。



以下总结了 COBIT 5 的主要变化和它们可能如何影响实施。

新的 GEIT 原则:

- 注重促成因素

——除了熟悉的流程实施模型, COBIT 5 还为有效的 GEIT 介绍了注重促成因素的要求。这些额外的促成因素也引用了第二章描述的 COBIT 5 流程。

- 新的流程参照模型

——COBIT 5 是建立在修改的流程模型基础上具有一个新的治理域和覆盖企业活动端到端的几个新的和修改的流程, 如业务和 IT。COBIT 5 合并 COBIT4.1, VAL IT 和 Risk IT 到一个框架, 且已修改的与目前的最佳实践保持一致。新的模型也可用作指导调整, 如必要, 企业自身的流程模型。

- **新的和修改的流程：**

——COBIT 5 介绍了五个新的治理流程，利用和改进 COBIT4.1, Val IT 和 Risk IT 治理方法和有助于进一步完善和加强执行-管理-水平 GEIT 实践融合现有企业治理实践且符合 ISO/IEC 38500。

-COBIT 5 已阐明管理-水平流程和整合 COBIT4.1, Val IT 和 Risk IT 内容到一个模式。

COBIT 5:启用流程在附录 A 提供了全部的交叉参照。有几个反映目前意见的新的和修改的流程，特别是：

AP003: 管理企业架构

AP004: 管理创新

AP005: 管理投资组合

AP006: 管理预算和成本

AP008: 管理关系

AP013: 管理安全

BAI05: 管理组织的变革启动

BAI08: 管理知识

BAI09: 管理资产

DSS05: 管理安全服务

DSS06: 管理业务流程控制

-COBIT 5 流程现在覆盖了端到端业务和 IT 活动，如完整的企业级视角。它提供了更全面和全覆盖反映普遍企业 IT 使用特征的实践。它使业务利益相关者的参与、责任和职责清晰和透明。

- **实践和活动：**

-COBIT 5 治理或管理实践等同于 COBIT4.1 控制目标和 Val IT 及 Risk IT 流程。

-COBIT 5 活动等等同于 COBIT4.1 控制实践和 Val IT 及 Risk IT 实践。

-COBIT 5 整合和更新所有以前的内容到一个新模型，具有一致的细节层次，COBIT 5:启用流程提供了所有的指南，使它在实施改进时更易于用户了解和使用资料。

- **目标和指标：**

-COBIT 5 继承了一样的目标和指标概念，如 COBIT4.1, Val IT 和 Risk IT，而这些命名为企业目标、IT 相关目标和流程目标，反映了企业级视角。

-COBIT 5 现在提供了以企业目标驱动 IT 相关目标为基础修订的目标级联，其次是支持关键流程。这类似于 COBIT4.1 的目标级联，具有更新的一组目标和关系及更详细的主要和次要关系。这种级联仍然是建立战略调整和重要流程范围的关键工具。

-COBIT 5 提供了企业目标和指标的实例，流程和管理实践级别。这与只有一个级别较低的 COBIT 4.1, Val IT and Risk IT 不同。

- **输入和输出：**

-COBIT 5 为每个管理实践提供了输入和输出(活动)，而 COBIT4.1 只在流程级别提供这些。这为设计流程提供了额外的详细指导，包括必需的工作产品和有助于输入流程整合。

- **RACI 图：**

-COBIT 5 提供 RACI 图描述角色和职责与 COBIT 4.1, Val IT and Risk IT 类似的方法。

-COBIT 5 为每个管理实践提供了比 COBIT4.1 更完整、详细和清晰的通用业务和 IT 任务参与者的值域和图表，当设计和实施流程时促成更好地角色参与者职责定义或参与级别。

- **流程能力成熟模型和评估(参考实施生命周期阶段 2 和阶段 3 讨论的)**

-COBIT 5 中止了 COBIT 4.1, Val IT and Risk IT 能力成熟模型(CMM)- 基于能力成熟模型方法，和现在支持新的基于 ISO/IEC 15504 的能力评估图。有关怎样完成能力自评估的

指南将会在计划的 COBIT 5 自评指南中提供。

以下概述了怎样基于标准完成差距分析：

● 识别和优先排序的改进领域(如：阶段 3 概述)鉴于以下：

- 识别优势、劣势和风险
- 企业目标
- 提高客户满意度的条件
- COBIT 5 指南和其它相关标准和最佳实践
- 为评估结果提供基本比较框架基准
- 现有流程绩效目标和指标，可以表明驱动改进的根本原因
- 没有实现陈述改进目标的风险

● 分析评估优势和劣势：

-确认优势，如最高流程能力水平等级的流程。考虑到：

- 可以采用的和机构化的良好实践经验
- 提高相关流程有效性的条件

-确认劣势而来源于：

- 低水平流程属性等级
- 缺少需要实现流程目的实践的流程(考虑 COBIT 5 管理实践和活动和其它促成因素以及相关标准和最佳实践)
- 需要实现具体企业目标能力水平中失衡的流程属性等级

-在一组评估流程内低水平流程属性等级也许指出了具体流程类型的劣势(如，低于流程能力水平 2 的级别显示了在管理和支持流程类型的劣势)

-同样的，应比较相关流程的流程属性等级。改进活动就需要纠正任何不平衡。

COBIT 4.1, Val IT 和 Risk IT 基于 CMM 方法不兼容 COBIT 5 ISO/IEC 15504 方法，因为用不同的属性测定级别。COBIT 5 方法被 ISACA 认为是更强大的、可靠的和可重复的而且也将支持鉴定评估者的正式评估，促使企业获得独立的和符合 ISO/IEC 标准的认证评估。

COBIT 5 第八章提供了新 COBIT 5 流程能力模型和比较目前在 COBIT 4.1, Val IT and Risk IT 使用方法的全面描述。

COBIT 4.1, Val IT and Risk IT 用户希望迁移到新 COBIT 5 方法将需要重新调整他们目前的级别，采用和学习新的方法，开始一套新的评估取得新方法的收益。虽然从目前的评估收集了一些信息可能可再度使用，但在迁移这些信息时仍需注意，因为在需求上有明显差别。

COBIT 4.1, Val IT and Risk IT 用户希望继续使用基于 CMM 的方法，无论是作为临时的还是永久的方法，都可以使用 COBIT 5 指南，但必须使用 COBIT 4.1 通用属性表而不是高级别成熟模型。提纲形式的程序如下：

1. 比较 COBIT 5 治理或管理实践流程范围和确定任何差距的活动(假设已接受管理和同意 COBIT 5 指南的全部范围)。为达到级别 3(定义级)和更高，所有的实践应已处理。
2. 比较详细的流程中 COBIT 4.1 成熟属性表(附录 E)和评估每个属性达到的级别。除此之外，当评估每个属性时考虑如何做好以下被广泛应用的 COBIT 5 流程指导：

- 意识和沟通-EDM01.02 和 AP001.04
- 政策、计划和程序- EDM01.02, AP001.03 和 AP001.08
- 工具和自动化- AP003.02
- 技能和专业知识-AP007.03
- 职责和责任-流程 RACI 图和 EDM01.02 及 AP001.02
- 目标设定和衡量方法-AP007.04 和 MEA01

3. 比较任何有效的基准和模型可能存在检查评估的合理性

4. 设定整体成熟度水平的最低属性级别(除非属性不被视为实质上有意义的流程能力)，同时也考虑治理或管理实践的覆盖范围。全部使用数字等级而不是“之间”或百分比。只有一个级别的所有属性都满足时才能获得相应的级别。管理者需要一个是否有助改进的透明的和实际的视图。

5. 分析目前和目标级别的差距，通过各方面考虑目前流程的优势和劣势，比较 COBIT 5 治理或管理实践和活动指导，COBIT 5 促成因素，和其它相关的标准和最佳实践。

计划和范围

COBIT 5 和这指南的配套资料提供了一个理解业务和治理优先级及需求的有效方法，这些理解可在实施治理和管理启动时使用。这种方法也提高了为治理改进准备的业务模式，获得利益相关者的支持，和预期收益的实现和监控。

这种关系可以用从上自下的方式描述。COBIT 5 有助于保证战略调整和驱动做什么，支持由企业目标到 IT 相关目标到 IT 流程的级联，进一步的说明如下：

- 企业目标
- 治理和管理需求
- 关键的 IT 流程
- 优先治理或管理实践和活动

目前利益相关者需要对 GEIT 进行明确评价(如第三章描述的，图像和图 7 及 COBIT 5 涉及到的)和目前企业目标及它们是如何影响 GEIT 的非常有用的三个原因：

- 利益相关者要求和企业目标影响需求及 GEIT 的优先级。如，有可能是注重成本降低，符合性或推出新的业务产品，在目前治理优先排序上每一个都可能处于不同的重点。
- 利益相关者要求和企业目标有助于关注在改进 GEIT 时哪些应给予留意。

COBIT 5 为定义企业和 IT 相关目标和它们之间的相互关联提供了有用的指南和实例。一组通用企业目标和 IT 相关目标级联显现在 COBIT 5 和 COBIT 5：启用流程。这些实例促使 COBIT 用户关联他们的企业目前业务和具体目标的 IT 环境，然后映射到可能关系到成功实现这些目标的流程。

绩效测量

良好治理的一个很重要的原则是应提供一个明确定义和沟通目标的管理，其次应用适当的做法管理目标。用指标监控绩效促进管理确保目标实现。

- 有助于业务和 IT 职能增加企业价值机遇的远期规划做得更好。

COBIT 5 企业和 IT 相关目标是作为 IT 目标设定和建立绩效衡量框架的基础。IT 目标作为目标应与企业目标保持一致。COBIT 5 提供了在三个层面定义目标结构：企业、IT 总体和 IT 流程。这些目标通过已知的效果测量进行衡量，因为它们测量期望目标的效果。具体层次的度量指标也作为实现较高层次目标的绩效驱动。这些目标和度量指标可用于设立目标和通过建立记分卡监控绩效及驱动改进的绩效报告。

COBIT 5 提供有关如何定义和分解业务目标及建立基于 BSC 的监控指标的指南。

治理和管理实践和活动

COBIT 5 阐明了治理和管理实践之间的区别，具有额外新的治理领域。COBIT 5 框架提供了有关企业治理和管理之间差异的说明。以 COBIT 5 为基础设计的流程和程序应总是适合企业的文化，管理方式和 IT 环境的要求。必须适当调整以适应 COBIT 5 中的指南。建议采用已介绍的最佳实践，

而且适应它们以便它们将实用和适合每个具体企业的目标和要求。活动提供了关于实现具体管理实践必须实施什么的指导。

COBIT 5 实践和活动是以目前相关的标准和可充分利用以获得更多详细指导的最佳实践为基础。

角色和职责

对于每个流程，COBIT 5 提供了实例 RACI 图指明了谁是执行或负责，而谁需要商议或一系列有代表性角色参与者流程活动的告知(端到端，业务和 IT)。角色参与者可以是个人(如 CFO 或运营总监 COO)或组织结构(如董事会或企业风险委员会)。明确执行和责任是 GEIT 很重要的原则。这些图可用作定制 IT 流程具体 RACI 图的基础。

附录 A:映射核心问题到 COBIT 5 流程

图案 4 显示了 COBIT 5 中全部 37 个治理和管理流程。根据早前描述的流程模型，所有流程的详细资料包含在 COBIT 5：促成流程。



图 45 提供了核心问题的实例(如第三章讨论的)和选定作为这些核心问题相应指导的 COBIT 5 流程实例。

图 45-核心问题映射到 COBIT 5 流程	
经营挫折因失败的举措，增加了 IT 成本和低业务价值的认知	EDM02, AP001, AP002, AP005, AP007, BAI01, BAI02
与 IT 相关业务风险有关的重大事件，如数据丢失或项目失败	EDM03, AP009, AP012, DSS 域
外包服务交付问题，如商定的服务水平始终没有得到满足	EDM04, AP009, AP010
不符合法规或合同要求	EDM03, MEA03
IT 限制了企业的创新能力和业务灵活性	EDM04, AP002, AP004
关于缺少 IT 绩效或 IT 服务质量问题报告的定期审计结果	MEA02
隐藏和欺诈的 IT 开销	EDM02, AP005, AP006
新计划或新措施的重复或重叠，或资源浪费	EDM02, EDM04, AP005, BAI01
不充足的 IT 资源，人员技能不足或人员精力不足/不满	EDM04, AP007
IT 启用的变革经常不能满足业务需要且交付延迟或超出预算	AP002, AP005, BAI01
多重和复杂的 IT 保证投入量	MEA02
董事会成员或高级管理层不愿意参与到 IT，或缺乏承诺和满意的 IT 业务支持	EDM01, EDM02, AP001, AP002
复杂的 IT 运营模式	EDM01, AP001, AP002, MEA02

附录 B:决策矩阵实例

图 46-决策矩阵实例		
决策主	范围	执行、责任、商议和告知(RACI)

题		执行委员会	IT 战略委员会	安全委员会	方案指导委员会	项目指导委员会	IT 经理	业务经理	员工
治理	<ul style="list-style-type: none"> 保持与企业治理一致 建立原则、结构和目标 	A/R	R	C			C	R	I
业务战略	<ul style="list-style-type: none"> 确定企业目的和目标 决定 IT 在哪和怎样能够促进和支持业务目标 	A/R	R	C			C	R	I
IT 政策	<ul style="list-style-type: none"> 提供准确的、可理解的和认可的政策、程序、指导方针和其它利益相关者文档 制定和推出 IT 政策 执行 IT 政策 	I	A	C			R	C	C
IT 战略	<ul style="list-style-type: none"> 在业务需求转换到服务提供时结合 IT 和业务管理，且制定战略以透明和有效的方式交付这些服务。 从事业务和高级管理层调整 IT 战略规划与当前和未来的业务需求。 了解目前的 IT 能力 为量化的业务需求的业务目标提供优先处理计划 	I	A	C	I		R	C	C
IT 技术方向	<ul style="list-style-type: none"> 为业务应用提供合适的平台符合定义的 IT 架构和技术标准。 制定与技术基础设施一致的技术获取计划。 设计基础设施维护 	I	C	C			A/R	C	C
IT 方法和框架	<ul style="list-style-type: none"> 建立透明的、灵活的和响应的 IT 组织结构及定义和实施整体所有者、角色和职责到业务和决策过程的 IT 流程。 定义一个 IT 流程框架 建立恰当的组织团体和结构 定义角色和职责 	I	C	C	I	I	A/R	I	I
企业架构	<ul style="list-style-type: none"> 定义和实施，架构和认可和影响技术条件的标准 建立一个指导架构和验证符合性的专题论坛 建立一个兼顾成本、风险和需求的架构计划 定义信息架构，包括含有数据分类方案的企业数据模型的建立 确保信息架构和数据模型的准确 分配数据所有权 应用商定的分类方案分类信息 	A	C	C	I	I	R	R	C

图 46-决策矩阵实例(续)

决策主题	范围	执行、责任、商议和告知(RACI)						
		执行委员会	IT 战略委员会	安全委员会	方案指导委员会	项目指导委员会	IT 经理	业务经理
IT 能力投资和投资组合优先顺序	<ul style="list-style-type: none"> 形成有效和高效的 IT 能力投资和投资组合决策 预测和分配预算 确定正式的投资准则 衡量和评估预测的业务价值 	I	A		C	C	R	
IT 能力投资和方案优先顺序	<ul style="list-style-type: none"> 设定和追踪符合 IT 策略和投资决策的 IT 预算 衡量和评估预测的业务价值 确定方案和适用于 IT 项目和促使利益相关者参与及监控项目风险和进展的项目管理方法 确定和执行方案和项目框架及方法 发布项目管理指南 完成在项目组合中每个详细项目的项目规划 	I	A		R	C	C/I	C/I
管理、监控和评价 SLAs	<ul style="list-style-type: none"> 识别服务需求，商定服务水平和监控服务水平的实现 正式化符合需求和交付能力的内外部协议 报告服务水平业绩(报告和会议) 识别和沟通新的和更新的战略规划服务需求 满足预定数据流程的运营服务水平，保护敏感输出，监测和维护基础设施 	I	A	R			R	R
IT 应用管理	<ul style="list-style-type: none"> 确认技术可行性和成本-有效性解决方案 明确业务和技术需求 以开发标准确定可行性研究报告 批准(或拒绝)要求和可行性研究报告 确保有一个及时的和成本-有效性的开发流程 业务需求转化为设计规格 对所有的修改坚持开发标准 隔离开发测试和运营活动 	I	I	C			A/R	C
IT 基础设施管理	<ul style="list-style-type: none"> 运营的 IT 环境符合商定的服务水平和定义的说明 维护 IT 基础设施 	I	I	C			A/R	C
IT 安全	<ul style="list-style-type: none"> 定义 IT 安全政策，计划和程序及监 	I	A	R			R	R

	控、检测，报告和解决安全漏洞和事件 • 按照业务需求和影响了解安全需求，漏洞和威胁 • 以标准方式管理用户身份和授权 • 定期安全测试								
--	--	--	--	--	--	--	--	--	--

图 46-决策矩阵实例(续)

图 46-决策矩阵实例 (续)									
决策主题	范围	执行、责任、商议和告知 (RACI)							
		执行委员会	IT 战略委员会	安全委员会	方案指导委员会	项目指导委员会	IT 经理	业务经理	员工
采购和合同	<ul style="list-style-type: none">· 获取和维护 IT 资源响应交付战略，建立统一的和标准化的 IT 基础设施，降低 IT 采购风险。· 获得专业的法律和合同建议· 确定采购程序和标准· 采购需要的硬件、软件和服务符合已定义程序	I	I	C			A/R	C	C
IT 合规	<ul style="list-style-type: none">· 识别所有适用的法律，法规和合同及 IT 合规的相应级别，优化 IT 流程以降低非合规的风险· 确认与 IT 相关的法律、法规和合同的要求· 评估合规要求的影响· 监测和报告这些要求的合规性	C/I	A	C			A/R	C	C/I

附录 C:映射风险情景实例到 COBIT 5 流程

图 47-风险情景和 COBIT 5 流程能力

风险情景		COBIT 5 流程能力
如果情景是相关的和固有的最可能……	……给出这些负面的实例……	考虑这些 COBIT 5 流程是否需要改进。注意：在这列中，旁边的每个流程编号是考虑的流程实例。这些不是流程名称。
收益/价值实现风险		
IT 方案选择	<ul style="list-style-type: none"> 选定不恰当的方案实施和与企业战略和优先顺序不一致 在不同的新计划和新措施间重复 新的和重要的方案建立长期不适应企业架构 	<ul style="list-style-type: none"> AP002 调整业务和 IT 战略 AP003 适应企业架构 AP004 识别创新机会 AP005 投资组合管理决策 BAI01 方案管理计划和协调
新技术	<ul style="list-style-type: none"> 未能及时地采用和利用新技术(如功能, 优化) 新的和重要的技术发展趋势未确定 未能使用技术来实现预期结果(如未能形成需求业务模式或组织的变革) 	<ul style="list-style-type: none"> EDM04 资源管理指导和/或视角 AP002 战略识别技术机会 AP003 企业架构与目前技术发展趋势保持一致 AP004 新的和重要技术发展趋势识别 BAI02 具有使用新技术确定新业务模式的能力 BAI03 采用和利用新技术
技术选择	<ul style="list-style-type: none"> 实施选择了不适当的技术(如成本、性能、特点和兼容性) 	<ul style="list-style-type: none"> AP002 有效的战略技术选择 AP003 企业架构技术一致性 BAI03 确定和建立解决方案 AP013 技术选择的安全性影响
IT 投资决策形成	<ul style="list-style-type: none"> 业务经理或代表没有参与有关新的应用, 优先顺序或新技术机遇的重要的 IT 投资决策形成 	<ul style="list-style-type: none"> EDM02 价值管理指导和/或视角 AP002 IT 战略规划的业务参与 AP003 投资适合目标企业架构 AP005 投资组合管理决策 AP006 投资监控 AP008 认知业务期望值和利用 IT 的机会 BAI01 方案管理阶段方式
IT 问责制	<ul style="list-style-type: none"> 业务不承担那些它应承担的 IT 领域的责任, 如功能需求, 开发优先事项和评估新技术 	<ul style="list-style-type: none"> EDM01-05 高级管理层 IT 相关决策责任 AP001 业务和 IT 相关角色和职责 AP009 明确和批准的服务协议 AP010 定义和管理供应商协议和关系 BAI05 促进涉及 IT 责任和 GEIT 的组织变革
IT 项目终止	<ul style="list-style-type: none"> 项目由于成本、延期、范围蔓延或变更业务优先级没有以及时方式终止 	<ul style="list-style-type: none"> EDM01GEIT 政策、组织结构和角色 EDM02 价值治理监测 EDM04 资源治理监测 BAI01 方案项目管理阶段-方式 AP005 有效的投资组合管理决策形

		成 <ul style="list-style-type: none"> ● AP006 投资监测 ● MEA01 绩效监测
IT 项目经济	<ul style="list-style-type: none"> ● 单独的项目预算超支 ● 连贯的和重要的 IT 项目预算超支 ● 缺少投资组合和项目经济的意见 	<ul style="list-style-type: none"> ● EDM01GEIT 政策、组织结构和角色 ● EDM02 价值治理监测 ● EDM04 资源治理监测 ● AP006 投资监测 ● BAI01 方案项目管理计划和监控

图 47-风险情景和 COBIT 5 流程能力(续)

风险情景		COBIT 5 流程能力
如果情景是相关的和固有的最可能……	……给出这些负面的实例……	考虑这些 COBIT 5 流程是否需要改进。注意：在这列中，旁边的每个流程编号是考虑的流程实例。这些不是流程名称。
方案/项目交付风险		
架构的灵活性和适应性	<ul style="list-style-type: none"> ● 复杂的和不适应的 IT 架构阻碍了更进一步的发展和扩展 	<ul style="list-style-type: none"> ● AP001 高效的和确定的业务和 IT 相关流程 ● EDM04 在资源优化上的治理 ● AP002 响应战略规划 ● AP003 企业管理架构维护 ● AP004 创新和变革措施 ● BAI02 投资组合管理决策获得 ● BAI02, 03 调整开发生命周期方法 ● AP013 在一个灵活的和多变的环境保持安全性
IT 与业务流程的集成	<ul style="list-style-type: none"> ● 广泛的依赖和终端计算机的使用和重要信息需要的初级解决方案 ● 独立的损和非整合的支持业务流程的 IT 解决方案 	<ul style="list-style-type: none"> ● EDM01GEIT 政策、组织结构和角色 ● AP001 业务和 IT 相关角色和职责 ● AP002 调整业务和 IT 战略 ● AP003 架构设计和决策 ● AP008 业务和 IT 关系 ● BAI02 明确和理解业务需求 ● BAI03 适应新 IT 解决方案的业务流程 ● BAI05 管理有关 IT 的组织变革
软件实施	<ul style="list-style-type: none"> ● 当开始运行新软件时出现差错 ● 用户不准备使用和利用新的应用软件 	<ul style="list-style-type: none"> ● AP011 一致和有效的质量管理活动 ● BAI01 项目管理 ● BAI02 需求定义 ● BAI03 解决方案制定 ● BAI05 管理与软件实施有关的组织变更 ● BAI06 变更管理 ● BAI07 广泛的解决方法测试 ● BAI08 知识支持
项目交付	<ul style="list-style-type: none"> ● 内部开发部门偶尔地延迟 IT 项目交付 ● IT 项目交付中惯常地重大延误 ● 外包 IT 开发项目中过度地延误 	<ul style="list-style-type: none"> ● EDM01GEIT 政策、组织结构和角色 ● EDM02 价值治理监测 ● AP006 投资监测 ● BAI01 方案/项目管理计划和监控
项目质量	<ul style="list-style-type: none"> ● 由于软件、文档或功能需求的符合性达不到项目交付成果的质量 	<ul style="list-style-type: none"> ● AP003 架构标准 ● AP011 一致和有效的质量管理活动 ● BAI01 方案/项目管理计划和监控
服务交付/IT 运行风险		
基础设施技术	<ul style="list-style-type: none"> ● 淘汰的 IT 技术不能满足新业务 	<ul style="list-style-type: none"> ● EDM04 资源管理指导和/或视角

状况	需求, 如网络、安全和存储	<ul style="list-style-type: none"> ● AP002 识别和战略性地解决目前 IT 能力问题 ● AP003 维护企业架构 ● AP004 识别重要的技术发展趋势 ● BAI03 维护基础设施 ● BAI04 计划和解决能力及性能问题 ● BAI09 维护资产
应用软件的时效处理	<ul style="list-style-type: none"> ● 应用软件太老, 文档资料不全, 维护成本过高, 难于扩展或没有集成在目前架构中 	<ul style="list-style-type: none"> ● EDM04 资源管理指导和/或视角 ● AP002 识别和战略性地解决目前 IT 能力问题 ● AP003 维护企业架构 ● AP004 识别重要的技术发展趋势 ● BAI03 维护应用程序 ● BAI09 维护资产 ● DSS06 业务流程控制

图 47-风险情景和 COBIT 5 流程能力(续)

风险情景		COBIT 5 流程能力
如果情景是相关的和固有的最可能……	……给出这些负面的实例……	考虑这些 COBIT 5 流程是否需要改进。注意: 在这列中, 旁边的每个流程编号是考虑的流程实例。这些不是流程名称。
服务交付/IT 运行风险(续)		
合规	<ul style="list-style-type: none"> ● 不符合财务或生产的规章 	<ul style="list-style-type: none"> ● EDM01GEIT 合规政策和作用 ● AP001 合规政策和指导 ● AP002 合规需求计划 ● BAI02 识别和定义合规需求 ● MEA03 监控合规需求和目前情况
第三方供应商选择/绩效	<ul style="list-style-type: none"> ● 供应商支持和服务交付不足, 不符合 SLAs ● 大规模, 长期外包协定的外包商绩效不足 	<ul style="list-style-type: none"> ● AP010 有效的供应商选择、管理和关系 ● BAI03 有效的采购管理
基础设施失窃	<ul style="list-style-type: none"> ● 盗窃笔记本电脑的敏感数据 ● 盗窃开发服务器的大量重要内容 	<ul style="list-style-type: none"> ● AP001 资产保护的政策和指导 ● AP007 新员工和承包商的参与资料和背景调查 ● BAI03 在维护活动期间保护重要的资产 ● DSS05 物理安全措施
基础设施破坏	<ul style="list-style-type: none"> ● 由于破坏或其他原因破坏数据中心 ● 意外破坏个人笔记本电脑 	<ul style="list-style-type: none"> ● DSS01 环境保护和设备管理 ● DSS05 物理安全措施
IT 职员	<ul style="list-style-type: none"> ● 离职或长期不适用的关键 IT 职员 ● 关键开发团队离开企业 ● 没有能力聘用 IT 职员 	<ul style="list-style-type: none"> ● AP007IT 职员资源的发展和留用 ● BAI08 隐性知识管理
IT 经验和技能	<ul style="list-style-type: none"> ● 缺乏或不匹配 IT 相关技能因 IT 新技术或其它情况 ● 缺乏了解业务的 IT 职员 	<ul style="list-style-type: none"> ● AP007 定义和制定业务和 IT 职员能力的要求 ● BAI08 知识支持
软件完整性	<ul style="list-style-type: none"> ● 故意的修改软件导致错误数据或欺诈行为 ● 无意的软件修改导致意外的结果 ● 无意的配置和变更管理错误 	<ul style="list-style-type: none"> ● BAI02 定义应用控制需求 ● BAI06 变更管理 ● BAI07 测试和验收实践 ● BAI10 配置数据 ● DSS05 访问控制 ● DSS06 业务流程控制

基础设施 (硬件)	<ul style="list-style-type: none"> ● 硬件组件的错误配置 ● 由于事故或其它原因损坏机房的关键性服务器 ● 有意损害硬件, 如安全设备 	<ul style="list-style-type: none"> ● BAI03 在维护活动期间保护关键的资产 ● BAI10 配置数据 ● DSS05 物理安全措施
软件性能	<ul style="list-style-type: none"> ● 关键的应用软件经常性的软件故障 ● 重要系统软件的周期性的性能问题 	<ul style="list-style-type: none"> ● BAI03 软件开发质量保证 ● BAI04 计划和处理能力和性能问题 ● DSS03 根本原因分析和问题解决
系统能力	<ul style="list-style-type: none"> ● 当用户数量增加时, 系统无法处理交易量 ● 当新的应用或部署新的计划时, 系统无法处理系统负载 	<ul style="list-style-type: none"> ● AP003 架构原理的可扩展性和灵活性 ● BAI03 维护基础设施 ● BAI04 计划和处理能力和性能问题
基础设施软件的时效处理	<ul style="list-style-type: none"> ● 使用不支持版本的操作系统软件 ● 使用旧的数据库系统 	<ul style="list-style-type: none"> ● EDM04 资源管理指导和/或视角 ● AP002 识别和战略性地解决目前 IT 能力问题 ● AP003 维护企业架构 ● AP004 识别新的和重要的技术发展趋势 ● BAI03 维护基础设施 ● DSS06 与业务流程控制相关的问题
恶意软件	<ul style="list-style-type: none"> ● 恶意软件入侵关键业务服务器 ● 笔记本电脑经常受到恶意软件感染 	<ul style="list-style-type: none"> ● AP001 软件使用的政策和指导 ● DSS05 恶意软件检测

图 47-风险情景和 COBIT 5 流程能力 (续)

风险情景		COBIT 5 流程能力
如果情景是相关的和固有的最可能……	……给出这些负面的实例……	考虑这些 COBIT 5 流程是否需要改进。注意: 在这列中, 旁边的每个流程编号是考虑的流程实例。这些不是流程名称。
服务交付/IT 运行风险 (续)		
逻辑攻击	<ul style="list-style-type: none"> ● 病毒攻击 ● 未授权用户企图非法进入系统 ● 拒绝服务攻击 ● 网站缺陷 ● 产业侦测 	<ul style="list-style-type: none"> ● AP001 IT 资产的保护和使用政策和指导 ● BAI03 解决方案的安全需求 ● DSS05 访问控制和安全监测
信息介质	<ul style="list-style-type: none"> ● 含有敏感数据的便携式介质的丢失/泄露 (如..CD, 通用串行总线 [USB] 设备, 便携式磁盘) ● 备份介质丢失 ● 由于未能遵循信息处理准则意外泄露敏感信息 	<ul style="list-style-type: none"> ● AP001 IT 资产的保护和使用政策和指导 ● DSS05, 06 保护移动和/或可移动存储及介质设备
公共事业设备性能	<ul style="list-style-type: none"> ● 周期性的公共事业设备故障 (如.., 电信、电力) ● 经常的, 长期的公共事业设备故障 	<ul style="list-style-type: none"> ● AP008 关键的公共事业设备供应商关系/管理 ● DSS01 环境保护和设施管理
产业行动	<ul style="list-style-type: none"> ● 由于劳工联合罢工难以接近设施和建筑物 ● 由于产业行动无法使用关键的职员 	<ul style="list-style-type: none"> ● AP007 人员关系和关键的人员 ● BAI08 管理人员知识
数据 (数据库) 完整性	<ul style="list-style-type: none"> ● 数据的有意修改 (如帐号, 安全相关数据, 销售数字) ● 数据库损坏 (如客户端或交易数据库) 	<ul style="list-style-type: none"> ● AP003 信息架构和数据分类 ● BAI03 开发标准 ● BAI06 变更管理 ● DSS01 管理数据存储

		<ul style="list-style-type: none"> ● DSS05 访问控制
逻辑非法入侵	<ul style="list-style-type: none"> ● 用户绕过逻辑访问权限 ● 用户获取访问未制授权信息 ● 用户窃取敏感数据 	<ul style="list-style-type: none"> ● AP001 IT 资产的保护和使用政策和指导 ● DSS05 访问控制和安全监控 ● AP007 合同人员政策
运营 IT 错误	<ul style="list-style-type: none"> ● 在备份、系统升级或系统维护期间运行错误 ● 错误的信息输入 	<ul style="list-style-type: none"> ● AP007 人员培训 ● DSS01 运行程序 ● DSS06 业务流程控制
合同执行	<ul style="list-style-type: none"> ● 未遵守软件版本协议(如.., 使用和/或销售无许可证的软件) ● 服务提供商的合同责任未能满足客户/顾客 	<ul style="list-style-type: none"> ● AP009 监测服务协议 ● AP010 供应商协议和关系监控 ● DSS02 软件许可证管理 ● MEA03 合同执行要求和目前情况监测
环境	<ul style="list-style-type: none"> ● 使用的设备不环保(如..., 高功率消耗, 包装材料) 	<ul style="list-style-type: none"> ● AP003 企业架构中包含环保原则 ● BAI03 解决方案的选择和采购原则 ● DSS01 环境和设施管理
自然行为	<ul style="list-style-type: none"> ● 地震 ● 海啸 ● 大风暴/暴雨 ● 大火灾 	<ul style="list-style-type: none"> ● DSS01 环境和设施管理 ● DSS05 物理安全 ● DSS04 管理持续性

附录 D:实例业务模式

注意: 这个实例提供了一个非规定性的通用指导鼓励业务模式的筹划以证明在 GEIT 实施方案中的投资。每个企业都会有自身改进 GEIT 的原因和筹划业务模式自身的方法, 一个可以从强调量化收益的详细方法到更高水平和定性的方法。企业应遵循现有的内部业务模式和投资定位方法, 如果它们存在, 且应用这个实例和发布的指南有助于关注的应解决的所有问题。制定业务模式的进一步指导可在 COBIT 5 流程 AP005 和业务模式指南: 使用 VAL IT2.0 中找到。

该实例情景是一大型跨国的企业, 具有传统的既定业务单位和采用最新技术的新的基于互联网业务的混合体。许多业务单位已获得和生存于不同的国家和不同的地方政治, 文化和经济环境。重要集团的行政管理已受到最新企业治理指南的影响, 包括已集中使用一段时间的 COBIT。他们想确定迅速扩张和在很多业务中采用先进 IT 将交付的预期价值和管理重大的新风险。因此他们授权整个企业采用统一的 GEIT 方法, 也包括审计的参与和风险的作用及所有实体适当控制的业务单元管理内部年度报告。

尽管实例来源于实际情况, 但不是特定现有企业的反映。

执行概要

该业务模式文档概述了基于 COBITAcme Corporation 提出 GEIT 方案的范围。

一个合适的业务模式需要确保 Acme Corporation 的董事和每个业务单位支持这个行动, 确定可能的收益而且监测业务模式以确保预期收益的实现。

构成 Acme Corporation 业务整体的范围包括一切。必须认可一些优先处理流程的形式将应用于由 GEIT 方案最初覆盖范围的所有实体，由于有限的方案资源。

有广泛的利益相关者对 GEIT 成果感兴趣，从 Acme Corporation 董事会到每个实体的地方管理者，以及外部利益相关者，如股东和治理机构。

需要考虑到已给出的一些重大挑战，以及风险，在 GEIT 方案实施中要求的全球规模。更多的挑战问题之一是互联网业务的许多企业因素特性，以及现有 Acme Corporation 中分散或联盟的业务模式。

GEIT 方案将通过侧重 Acme 流程能力和在 COBIT 中定义的，相关的各个业务单位关系到这些的其它促成因素实现。通过推进 GEIT 方案成员研讨会方法确定每个实体的重点接受相关的和优先的流程，从各个单位的业务目标，和 IT 相关业务风险情况开始到应用于具体的业务单位。

GEIT 方案的目的是确保恰当的治理结构到位和提高能力水平及相关 IT 流程的适当性，IT 流程能力的提高达到预期，相应的风险将成比例降低和提高效率和质量。这样，各个业务单位的真正业务效益就会实现。

一旦建立了每个业务单位的能力水平评估流程，预期的自评估将作为正常的业务实践持续在每个业务单位。

GEIT 方案将在两个不同阶段交付。第一个阶段是开发阶段，团队将开发和测试方法和用于 Acme Corporation 的工具组件。在阶段 1 结束时，结果将呈述给集团管理者作最终审批。一旦获得最终批准的改进的业务模式方式，GEIT 方案就会以一致的方式推入实体。

必须指出的是在每个业务单元实施补救行动确定它不是 GEIT 方案的责任。GEIT 方案只不过以统一的方式提供每个单元的进展报告。

由于 GEIT 方案需要解决的最后一个难题是以可持续方式向前报告结果。这问题将需要花费时间和大量的讨论及致力于它的发展，这将导致增加现有企业的报告机制和记分卡。

应制定 GEIT 方案开发阶段的最初预算。在单独的时间安排表详细的预算。详细预算应在项目阶段 2 完成和提交集团管理者审批。

背景(看第二章，定位 GEIT)

GEIT 是整个企业治理的组成部分和专注于 IT 绩效和管理因企业依赖 IT 的风险。

IT 已集成到 Acme Corporation 业务运行中和许多，特别是互联网业务，是业务的核心。GEIT 因此遵循集团分散方式的管理结构。每个分公司/业务单位的管理就是负责确保实施了与 GEIT 有关的正确流程。

每年，每个重大分公司的管理者需要提交正式的书面报告给合适的风险管理委员会，是董事会的了集，在财政年度期间实施了何种程度的 GEIT 政策。在每次安排的风险管理委员会会议上应报告重大的异常情况。

董事会，由风险和审计委员会协助，将保证集团 GEIT 绩效的评估、监测、报告和作为整体报告的一部分公开 GEIT 报告书。这样的报告书应根据风险、合规和内部审计团队和每个重大分公司的管理报告获得，提供相关的内外部利益相关者和关于集团的 GEIT 绩效质量的可靠信息。

内部审计服务将向管理者和审计委员会提供关于 GEIT 充分性和有效性的保证。

IT 相关业务风险将会报告和作为风险管理流程部分讨论，风险记录呈述给相关风险委员会。

业务难题(看第三章，第三节，导读一确定需要采取的行动：识别核心问题和触发事件)

由于 IT 的普遍特性和技术变化的步伐，需要一个可靠的框架适当地控制整个 IT 环境和避免控制缺陷可能会暴露企业不可接受的风险。

其意图不是阻碍各种业务实体的 IT 运行。相反的，它以一种方式提高实体风险评测形成业务方向与提供高质量的服务和效率，同时明确不仅遵循 Acme Corporation 集团 GEIT 章程，而且还应遵循任何其他立法，法规和/或合同要求。

面临的一些核心问题实例是：

- 结构复杂的 IT 保证投入量由于业务单元的许多与企业有点关的特性
- 复杂的 IT 运行模式由于其基于业务模式中使用的互联网服务
- 地理上分散的实体，由不同的文化和语言构成
- 分散/联盟和集团内使用的大量独立的业务控制模式
- 实施合理的 IT 管理水平，给出非常高的技术，有时 IT 劳动力的不稳定性
- 企业驱动创新能力和业务灵活性需要风险管理和具有适当控制的 IT 平衡
- 为每个业务单位确定风险和容忍的水平
- 不断增长的需要，侧重于满足监管(隐私权)和合同的(支付卡行业[PCI])合规要求
- 有关不足 IT 控制和报告 IT 服务质量问题的定期审计结果
- 在激烈的市场竞争下成功和按时交付新的和创新的服务

差距分析和目标

目前没有整个集团的方法或 GEIT 框架或 IT 最佳实践和标准的使用。在地方业务单元水平中有不同程度的采用与 GEIT 有关的良好实践。因此，很少有关关注传统上已付出的 IT 流程能力水平。根据经验，水平普遍较低。

GEIT 方案的目的是由此提高能力水平和 IT 相关流程的充足及每个业务单元控制的适当，以优先考虑的方式。

结果应是已确定和阐明重大的风险，和风险处理状况的管理及报告它的状况。为了提高每个业务单元的能力水平，因此每个实体评测的 IT 相关业务风险应减少和质量效率应成比例增加。最终有效 GEIT 的结果应是增加业务价值。

考虑供选择的方案

许多现有的 IT 框架，每个都试图带来了 IT 控制之下的具体问题。COBIT 框架被认为是世界领先的 GEIT 和控制框架。COBIT 框架已由集团的一些分公司实施。它也是 King III 报告中特别提及的作为 GEIT 实施的可能框架。

COBIT 是 Acme Corporation 选择作为 GEIT 实施首选的框架和由此被所有分公司采用。

COBIT 不必全部实施；只有那些具体分公司的相关领域或业务单元必须实施；考虑以下：

1. 在业务生命周期每个实体的开发阶段
2. 每个实体的业务目标
3. 业务单元 IT 的重要性
4. 每个实体面临的 IT 相关业务风险
5. 法律和合同的要求
6. 任何其它相关的原因

当其它框架已在具体的分公司或业务单元实施，或仍将在未来被实施时，这样的实施应被映射到 COBIT，为了报告、审计和内部控制的清晰度的理由。

提议解决方案

GEIT 方案在两个不同阶段计划

阶段 1. 准备-计划(看第三章. 迈出 GEIT 的每一步)

GEIT 方案的阶段 1 是开发阶段。在方案的这阶段期间，应开始进行以下步骤：

1. 风险管理支持和集团 IT 之间核心团队结构确定
2. 核心团队 COBIT 基础培训完成
3. 核心团队进行的研讨会确定了集团的方法
4. 在 Acme Corporation 建立一个在线社区用作知识共享的知识库
5. 识别所有利益相关者和他们的要求
6. 如果需要，分类和调整目前委员会结构，角色和职责，决策规则和报告约定
7. 制定和维护 GEIT 方案的业务模式作为成功实施方案的基础
8. 贯穿整个方案沟通计划的指导方针，政策和预期的效益，
9. 在方案的生命周期及之后使用的评估和报告工具的开发
10. 在一个地方实体方法的测试。为便捷的保证体系选择活动，和易于改进的方法和工具。
11. 在一个外地实体引导精确的方法。这是在更具挑战的业务环境下 GEIT 方案评估阶段难于理解和量化。
12. 最终业务模式和方法的提出，包括推出计划给 Acme Corporation 高级管理层审批

阶段 2. 方案实施(看第三章, 第二节. 应用一个持续改进的生命周期方法)

设计的 GEIT 方案开始进行持续改进的方案，基于以下这些步骤的重复的迭代生命周期：

1. 确定改进 GEIT 的驱动因素，来自 Acme Corporation 集团视角和业务单位层级
2. 确定目前 GEIT 状况
3. 确定 GEIT 的期望状况(短期和长期)
4. 确定在业务单位层级需要实施什么以实现本地业务目标，从而保持与集团期望一致
5. 在当地业务单位层级实施确定和商定的改进项目
6. 实现和监控收益
7. 支持新的工作方法保持推进的动力

方案范围

GEIT 方案将涵盖以下：

1. 所有集团实体图，然而，由于有限的方案资源，相互影响的实体应是优先的。
2. 优先排序的方法。它需要与 Acme Corporation 一致的管理，但可以依据以下完成：
 - a. 投资规模
 - b. 对集团的收益/贡献
 - c. 来自集团视角的风险概况
 - d. a 和 c 的结合
3. 在目前财务年度期间包含的实体列表。这还是有待确定和与 Acme Corporation 管理一致。

方案方法论和调整(看第六章. 实施生命周期任务、角色和职责)

GEIT 方案通过所有实体间使用互助、互动的研讨会方法达到它的要求。

方法起始于业务目标和目标所有者，通常为 CEO 和 CFO. 这种方法将会确保方案的结果，是接近一致地预期业务结果和优先级。

一旦已覆盖了业务目标，这时的重点就转移到 IT 运行，一般由首席技术官(CTO)或 CIO 控制，更进一步考虑详细的 IT 相关业务风险和目标。

业务和 IT 目标以及 IT 相关业务风险，这时结合在一个工具中(以 COBIT 指南为基础)将为业务单位所考虑的因素提供一系列重点领域的 COBIT 流程。在这种方式下，业务单位就能够优先补救尽力处理 IT 风险领域。

方案交付物(看第六章. 实施生命周期任务、角色和职责)

早期提到，GEIT 的整个目标是嵌入 GEIT 良好做法到各个集团实体的持续运营中。

由 GEIT 方案产生的具体成果是促使 Acme Corporation 衡量由 GEIT 方案交付的预期成果。这些包括以下：

1. GEIT 方案将通过网络平台促进企业内部知识共享，以及利用现有供应商对单独的业务单位的优势关系。
2. 将会建立的每个互助互相影响的业务单位的详细报告。报告将包括：
 - a. 目前优先的业务目标和随之基于 COBIT 的 IT 目标
 - b. 由业务单位以标准化的形式确定的 IT 相关风险，和基于 COBIT 流程和实践及其它提议的促成因素业务单位商定的专注的重点领域。
3. 有关由 GEIT 方案建立的 Acme Corporation 业务单位预期覆盖范围的整体进展报告。
4. 统一的集团报告将包括：
 - a. 正在进行的以监测一致的绩效指标体系的商定的实施项目业务单位的进展
 - b. 在 Acme Corporation 实体综合的 IT 风险视图
 - c. 风险委员会的具体要求
5. 有关方案预算与产生的实际花费总计的财务报告
6. 效益监测和对建立的业务单位定义的价值目标和指标报告

方案风险(看第五章. 促成变革)

以下被认为是 Acme Corporation GEIT 方案成功行动和持续成功潜在的风险类型。这些通过集中的变革启动将会降低，且通过方案审查和风险记录它们将会被监控和持续的处理。这些风险类型是：

1. 方案的管理承诺和支持，无论是集团层面以及地方业务单位层面
2. 通过采用方案，展示实际的价值交付和每个地方实体的收益。当地的实体应要采用交付价值的流程，而不是因政策到位而做。
3. 在方案实施中本地管理者的活动参与
4. 识别每个实体参与方案的关键利益相关者
5. IT 管理队伍的业务视角
6. 现有集团的任何治理或合规措施的成功整合
7. 恰当的委员会结构监督方案。例如：GEIT 方案的整体进展可能成为 IT 执行委员会的日常议程项目。地方等同的也需要设立。这是地理上可复制的，以及地方一级适当持股公司。

利益相关者(看第三章，第四节. 认识利益相关者的作用和要求)

以下确定的角色参与者作为在 GEIT 方案成果的利益相关者：

1. 风险委员会
2. IT 执行委员会
3. 治理团队
4. 执行人员
5. 地方管理者
6. 地方实体层级执行管理者(包括 IT 管理者)
7. 内部审计服务

最终的结构有角色参与者单独的名称在集团管理者商讨后将编制和公布。

GEIT 方案需要确定的利益相关者提供如下：

1. 指导 GEIT 方案的整体方向。这包括有关重大治理相关的议题, 根据 COBIT 指南定义集团 RACI 图, 以及设立优先级, 商议资金投入和满意的价值目标的决策。

2. 交付成果的验收, 和监测 GEIT 方案的预期收益。

成本-效益分析

方案应确定预期的收益, 和监测源自投资产生的真正业务价值。地方管理者应促动和支持方案。将产生如下收益的健全的 GEIT 将为每个业务单位建立具体的目标, 和监控及实施期间的测量确保实现收益:

1. 通过 IT 最大化业务商机的实现, 同时降低 IT 相关业务风险至可接受水平, 由此确保风险与所有业务活动机会的权衡。

2. 关键投资的业务目标的支持和这些投资的最佳回报, 由此 IT 活动和目标方向与业务战略保持一致。

3. 法律、法规和合同执行及内部政策和程序的遵守

4. 测量和监测进展、效率和效益的一致方法

5. 提高服务交付质量

6. 通过用更短的时间和更少的资源完成更多的一贯工作, 降低 IT 运行成本和/或提高 IT 生产力

主要的成本将包括集团方案管理的时间要求, 外部顾问资源和最初的培训内容。这些主要的成本在阶段 1 已估算。各个业务单位管理者和流程所有者为评估研讨会的费用将由地方提供资金和评估量提供。每个业务单位的具体项目改进活动在阶段 2 评估和以逐项考虑为基础再到整体。这将会促使集团最大化效率和标准化。

难题和成功因素(看第四章, 识别实施难题和成功因素)

图 48 总结了在方案实施期间可能影响 GEIT 方案的难题和应加以处理以确保成功结果的关键成功因素。

图 48-难题和 Acme Corporation 的计划行动

难题	关键成功因素-行动计划
无法获得和维持改进目标的支持	通过集团委员会结构缓解(同意和建立)
IT 和业务的沟通差距	所有利益相关者参与
改进成本超过预知的收益	注重效益识别
IT 和企业之间缺乏信任和良好的关系	<ul style="list-style-type: none"> ● 促进开放和透明的链接企业绩效管理的绩效沟通 ● 关注业务层面和服务意识 ● 确保 CIO 在建立信任和关系中的可信赖程度和领导作用 ● 规范化的经营治理角色和职责以便明确的决策问责制 ● 识别和沟通与提出改进有关的真正问题的解析, 需要避免的风险及获得的收益(用业务术语) ● 关注变革启动计划
负责 GEIT 方案的那些人缺乏顶点环境的了解	应用一致的评估方法
各层次的复杂性(技术、组织、运行模式)	在逐项处理基础上处理整体。从经验教训中获益和知识共享
了解 GEIT 框架, 程序和实践	培训和指导
抵制变革	确保实施生命周期也包括变革启动活动
通过改进	确保地方授权在整体水平
难以整合 GEIT 和外包合作伙伴的治理模式	<ul style="list-style-type: none"> ● 供应商/第三方参与 GEIT 活动 ● 在合同中加上条件和审计权
未能实现 GEIT 实施承诺	<ul style="list-style-type: none"> ● 管理期望值 ● 保持简单、实用和实效 ● 把整个项目分解为小的可实现的项目, 建立经验

	和效益。
试图同时做得太多。IT 处理过于复杂和/或费力的问题	<ul style="list-style-type: none"> ● 应用方案和项目管理原理 ● 使用里程碑 ● 优先处理 80/20 任务 (20%的努力获得 80%的收益) 而且以正确的次序仔细安排顺序, 实现速赢 ● 建立信任和信心; 有技能和经验保持简单和实用 ● 重用什么作为基础
IT 的救火模式和/或没有优先级和不能专注于 GEIT	<ul style="list-style-type: none"> ● 应用良好的领先技能 ● 获得承诺和驱使高级管理层因形成们有效的专注 GEIT ● 解决运行环境的根本原因 (外部干涉, IT 优先级管理) ● 应用严格的原则处理/管理业务请求 ● 获得外部协助
需要的 IT 技能和能力不到位, 如业务、流程、软技能的理解	关注变革启动计划: <ul style="list-style-type: none"> ● 开发 ● 培训 ● 辅导 ● 指导 ● 反馈到招聘流程 ● 交叉技能
改进不接受或应用	使用地方整体原则通过逐项方法。必须实际实施
效益难以表明或证明	确定绩效测量标准
失去兴趣和动力	建立集团级别的承诺, 包括交流

附录 E: COBIT4.1 能力属性表

图 49-COBIT4.1 能力表

意识和沟通	政策、计划和程序	工具和自动化	技能和专业经验	职责和责任	目标设立和衡量
1 需要认可出现的流程。 偶尔沟通的问题。	有流程和实践的初级方法。 流程和政策未定义。	一些工具可能存在; 使用基于标准的桌面工具。 没有计划要求工具使用。	流程技能要求不明确。 培训计划不存在和没有正式培训内容。	没有定义责任和职责。人们处理所有权问题基于被基础上的自主行为。	目标不明确和没有进行衡量
2 有需要采取行动的意识。 管理沟通的整体问题。	相似的和通用的流程出现, 但大部分是直觉因个人专业能力。 流程的一些问题是重复的因人员专业技能, 和一些文件和非正式了解政策和程序可能存在。	现有使用工具的一般方式只是基于解决开发的关键人员。 供应商工具可能已获取, 但是可能没有正确应用, 甚至可能只是作样子	关键流程明确最小的技能要求。 提供响应需要的培训, 而不是基于商定的计划, 且非正式地培训工作内容	个人承担自己的职责和通常拥有的责任, 尽管没有正式议定。当问题出现时, 责任是混淆的, 和存在指责倾向文化。	一些目标已设立: 一些财务衡量已建立, 但只有高级管理层知道。在单独领域有不一致的监测。
3 有了解需要采取的行动。 沟通中管理更正式和有结构。	形成使用良好的实践。 流程, 政策和程序已定义且所有关键活动已文档化。	计划已明确使用和标准化的工具到自动化的流程。 工具用作基本目的, 但可能与协定计划不一致, 且可能不相互融合	所有领域的技能要求已定义和文档化。 正式培训计划已制定, 但正式培训仍基于个人行为。	流程职责和责任已定义和流程所有者已明确。流程所有者不可能有全部授权来行使职责。	一些有效性目标和衡量指标已设立, 但没有沟通, 和有明确链接到业务目标。测量流程形成, 但不是一贯应用。

					IT 平衡记分卡概念已采用, 作为偶尔直观根本原因分析的应用程序
4 有了解完整的需求 应用成熟的沟通技术和使用标准的沟通工具	流程健全和完整, 采用内部最佳实践。流程的所有方面已记录和可重复。政策已得到认可和管理层的批准。采用和继承标准的开发和维护流程和程序	工具根据标准化计划实施, 且一些已和其它相关工具相互融合。工具已使用在主要领域, 自动化管理流程和监控关键活动和控制。	所有领域的技能要求已常规更新, 所有关键领域保证熟练, 且鼓励认证。根据培训计划采用成熟培训技术, 鼓励知识共享。所有内部领域专家参与, 评估培训计划的有效性	流程职责和责任可接受和工作方式促使流程所有者完全执行自己的职责。激励文化到位和激发积极的行动。	测量了效率和效果和沟通及链接到业务目标和 IT 战略目标。IT 平衡记分卡在一些领域异常情况管理者提醒已实施和根本原因分析已标准化。持续改进已形成。
5 有先进的, 前瞻性的了解需求 积极主动沟通基于现有趋势的问题, 应用成熟沟通技术, 且使用综合沟通工具。	应用外部最佳实践和标准。流程文件已逐步形成自动化工作流。流程、政策和程序是标准化的和集成促使端到端管理和改进	标准化工具组件已在整个企业使用。工具与其它相关工具已完全融合, 促使端到端支持流程。工具已用于支持流程改进和自动检测控制异常情况	组织正式鼓励持续提高技能, 基于明确的个人和组织的目标。培训和教育支持外部最佳实践和使用领先的理念和技术。知识共享是一个企业的文化, 和正部署知识库系统。外部专家和行业领先者作为指导。	流程所有者已授权制定决策和采取行动。职责的认可以一致的方式级联到组织。	有一个综合的绩效测量系统链接到 IT 绩效到业务目标通过 IT 平衡记分卡的全球应用。通过管理注意全球和一贯的异常情况和应用根本原因分析。持续改进是一种生命周期的方式。

九、联系我们:

汇哲科技—业内唯一信息安全专业培训服务机构!

网址: www.spisec.com

赞助: www.cncisa.org www.cncisa.com

商城: <http://spisec.taobao.com/>

地址: 上海黄浦区陆家浜路 1332 号南开大厦 1508

邮编: 200011

电话: 021-33663299

传真: 021-33663299-8002

邮箱: guomeng@cncisa.com