COBIT5 与 COBIT4.1 区别

一、 汇哲公司介绍

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；并在北京，广西等地区设立分部。其前身为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、信息系统审计等方面的培训和实践研究，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。

SPISE 为联合国训练研究所上海亚太地区经济和信息化人才培训中心汇哲信息安全培训部；（CIFAL Shanghai）是获得国家外事部门批复同意、由联合国训练研究所（UNITAR）与亚太地区城市信息化合作办公室（RCOCI）于 2006 年联合成立的面向亚太地区的国际培训机构。CIFAL Shanghai 是联合国训练研究所国际培训网络（CIFAL Network）在亚洲的成员单位。CIFAL 是“国际地方政府培训中心”的法语缩写。目前，联合国训练研究所已在全球设立了 12 个国际培训中心。这些培训中心均与所在地政府保持着十分良好的合作关系。每个联合国训练研究所人才培训中心是地方政府、国家中央政府、国际组织、私营部门和学术界间进行能力建设和知识共享的中心。汇哲科技主要从事信息安全与 IT 审计领域培训与后续服务保障工作。

SPISE 与网络信息安全管理与服务教育部工程研究中心，上海交通大学联合办学，共同建设与管理信息安全培训中心，并面向社会培养具备专业水平的信息安全专业人员，服务于政府和广大企业。该中心在上海张江园区拥有 10000 平方米实体场地。拥有密码与高性能芯片设计开发平台；网络防护性检测与攻防技术研究平台；全程全网内容安全综合监管平台；电子政务安全应用研发平台；信息安全社会化服务咨询平台等教学环境；信息安全攻防实验室。这些平台资源与课程体系等一起形成了独具特色的宽口径的信息安全实验教学体系。

SPISEC 为国内唯一一家以信息安全培训与后续服务为主的机构，整体培训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。

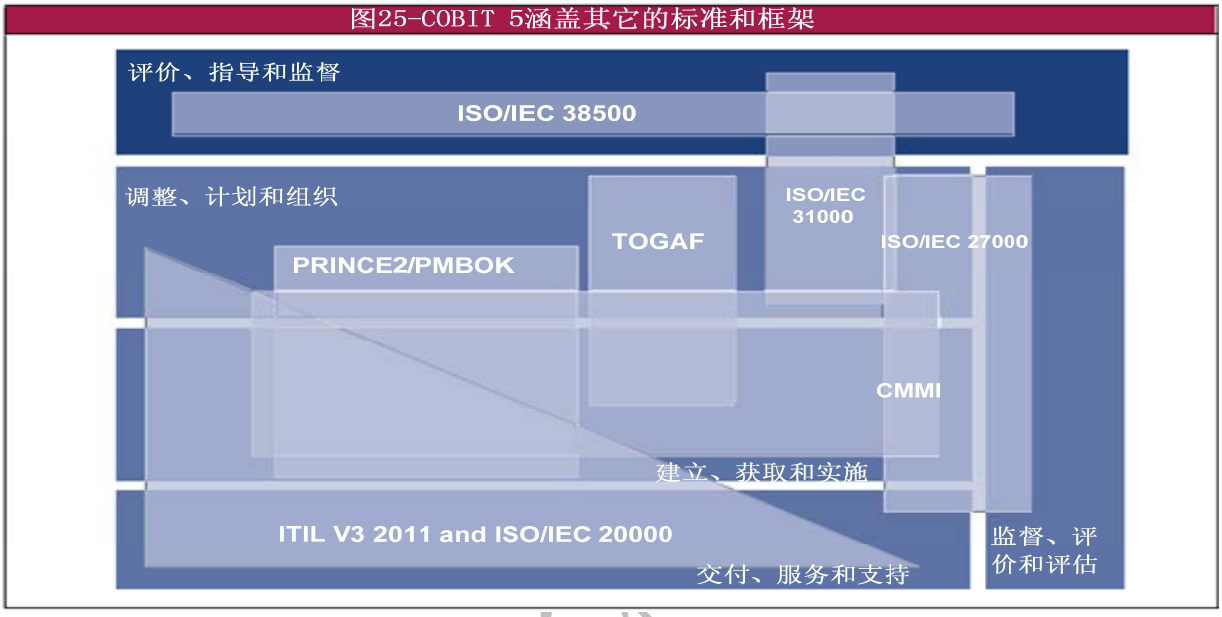
SPISEC于 2008 年开始在业内陆续组织多场专业知识学习讲座和研讨，并持续发布多期专业原创文档和学习形式期刊、书籍。SPISEC至今为 20000 多名会员提供免费的学习指导服务，其中为 3000 多名会员直接提供考试辅助、职业规划、学习计划梳理等服务，会员现分布央企、国企、金融、电信、移动、能源、制造、IT等多个行业。SPISEC的成立将更好地带动业内信息安全人员的培养和发展，保障国际信息安全学习联盟（www.cncisa.org）的基本运营，实现业内各领域有志之士的共同愿望，汇聚业内各领域的专业顶极人才。

二、 COBIT5 与COBIT4.1 的主要区别

（一）、集成了更多的框架和标准的应用

COBIT5 合并了 COBIT4.1 和 VAL IT 及 RISK IT 框架，并做了更新，兼容了目前众多的最佳实践和标准，如 ITIL、TOGAF…

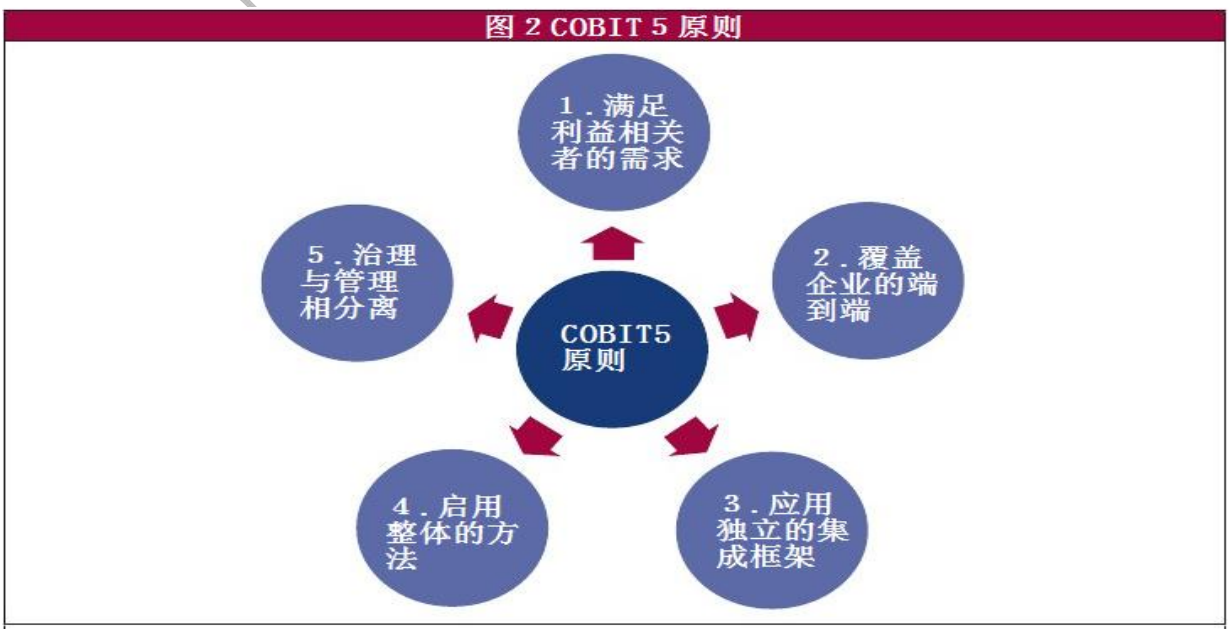
图25–COBIT 5涵盖其它的标准和框架



（二）、新的 IT 治理原则(五大原则)

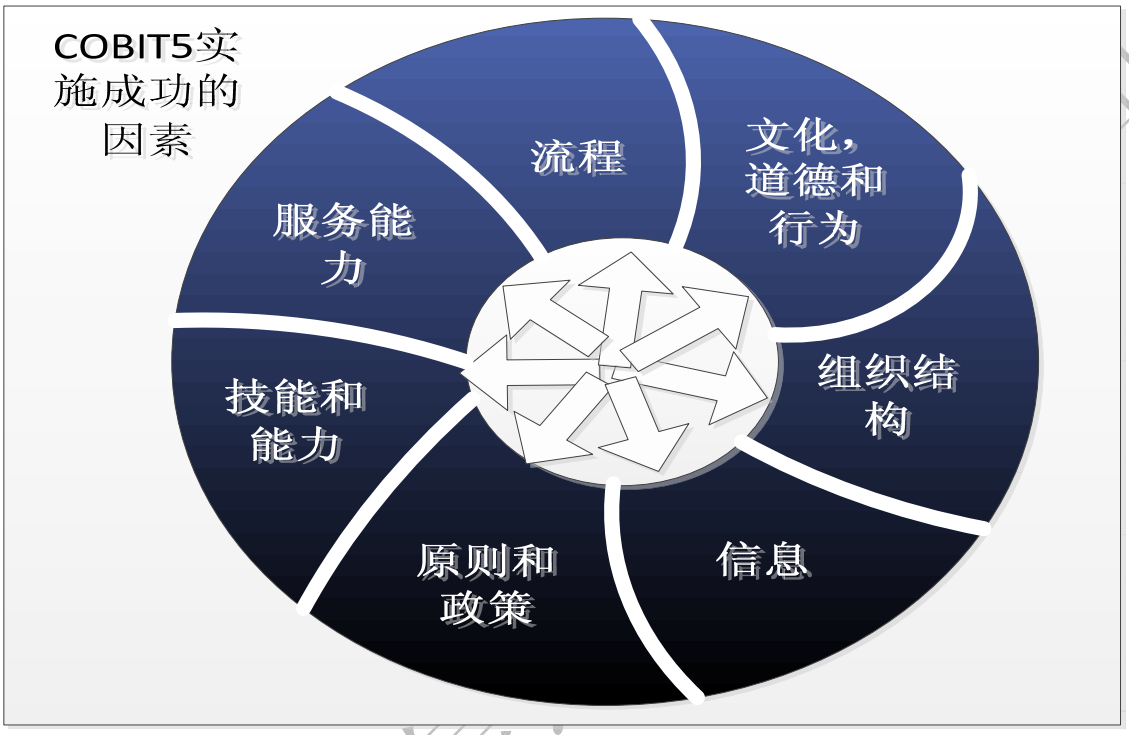
1、VAL IT 和 Risk IT 框架是原则的基础
2、更易于理解和应用于企业的环境，提供更有效的指导支持价值交付
3、利用了 ISO/IEC 38500 标准关于 IT 治理的六项原则来加固实现价值交付

图 2 COBIT 5 原则



（三）、更多的关注 IT 治理实施的促成因素(七大促成因素)：

1、COBIT4.1 没有促成因素，或未明确指明；
2、在 COBIT4.1 中，信息、基础设施、应用程序(服务)和人(人、技能和能力)属于资源
3、在 COBIT4.1 流程中很少提及原则、政策和框架
4、在 COBIT4.1 中流程是核心
5、通过责任、职责、商议和告知(RACI)角色和它们的定义说明组织结构
6、在 COBIT4.1 流程中也很少提及文化、道德和行为



（四）、更新和修订了企业的目标和级联的 IT 目标

1、COBIT4.1 的企业目标

COBIT4.1 企业目标		
财务视角	1	为 IT 保障业务投资提供良好投资回报
	2	管理 IT 相关业务风险
	3	改进公司治理和透明度
客户视角	4	改善客户倾向和服务
	5	提供有竞争力产品和服务
	6	建立持续和可用的服务
	7	对业务需求变更提供灵活快捷的响应
	8	完成服务交付的成本最优化
	9	为战略决策提供可靠的和有用的信息
内部流程视角	10	改善和维护业务流程的功能
	11	降低流程成本
	12	提供与外部法律、法规及合同的合规性

	13	提供与内部政策的符合性
	14	管理业务变更
	15	改善和维持运营和员工生产力
学习与成长视角	16	管理产品和业务创新
	17	获得和维持技能熟练的和上进的人

2、COBIT5 在利益相关方价值交付的基础上，将治理目标（价值创造）从三个维度（利益实现、资源优化、风险优化）进行分解，并将治理目标按照平衡计分卡从财务、客户、内部、学习和成长四个视角与企业目标和 IT 目标进行关联；提供了一组自身定义的企业通用目标，虽然不是很详尽，但大多数企业的具体目标可以很容易映射到一个或多个通用企业目标。

图 5—COBIT 5 企业目标

平衡计分卡维度	企业目标	与治理目的的关系		
		利益实现	风险优化	资源优化
财务	1．利益相关者的商业投资的价值	P		S
	2．竞争性产品和服务的组合	P	P	S
	3．业务托管风险（资产保护）		P	S
	4．遵循外部法律和法规		P	
	5．财政透明度	P	S	S
客户	6．以客户为本的服务文化	P		S
	7．商业服务的连续性和可用性		P	
	8．快速应对不断变化的业务环境	P		S
	9．信息化战略决策	P	P	P
	10．服务交付成本的优化	P		P
内部	11．业务流程的功能优化	P		P
	12．业务流程成本优化的	P		P
	13．业务托管变更计划	P	P	S
	14．业务和员工的工作效率	P		P
	15．遵循内部政策		P	
学习与成长	16．有技能和积极性的员工	S	P	P
	17．产品和业务创新的文化	P		

3、COBIT5 修订和更新了目标级联

4、目标和指标

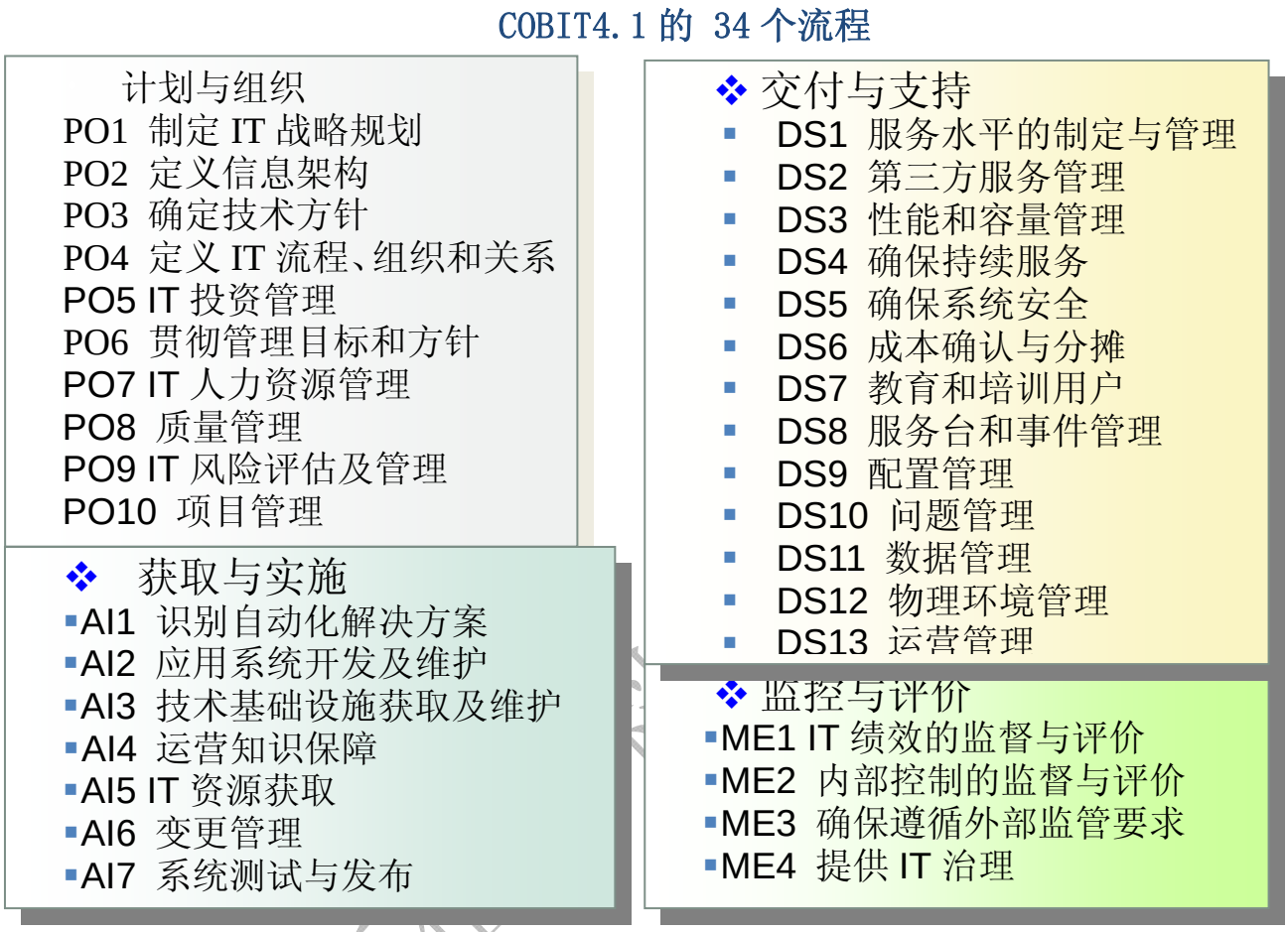
COBIT5 遵循与 COBIT4.1、Val IT 和 Risk IT 一样的目标和度量体系概念，但这些重新命名的企业目标、IT 相关目标和流程目标反映企业级视角。

5、COBIT5 依据企业目标驱动 IT 相关目标提供已修订目标级联，然后支持关键流程。

注：以上更多信息参阅汇哲 COBIT 5 企业 IT 治理和管理的业务框架中文版

（五）、区分了治理和管理的职能和控制流程

1、COBIT5 在原有 COBIT 4.1 的基础上也做了大幅调整



2、明确定义了治理和管理的职能和控制目标。

治理是 EDM（评价、指导、监督）

管理是 PBRM（计划、建立、运行、监测）

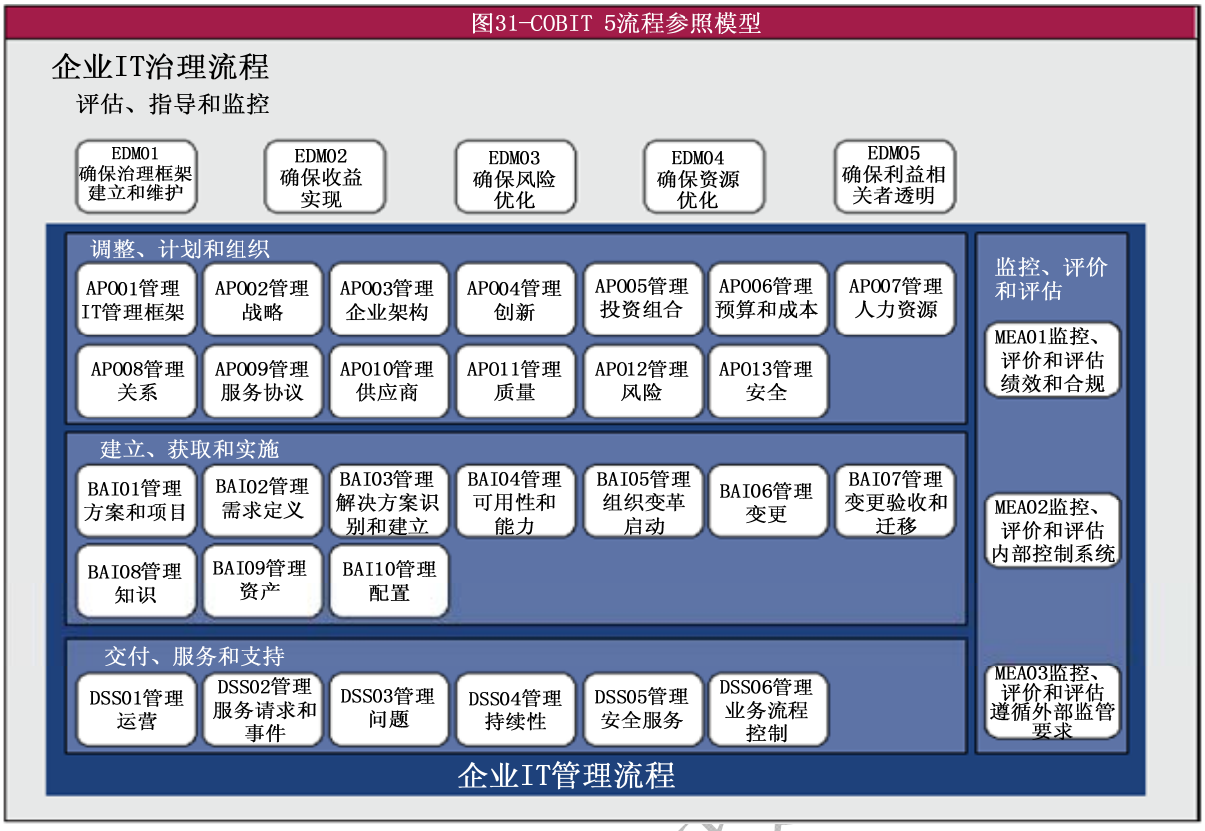
3、COBIT5.0 参照模型经过修订，具有一个新的治理域和一些新的和修改的流程；现在的 COBIT5.0 的参照模型覆盖了企业端到端的活动，如业务和 IT 功能域。

4、划分为两个主域：

(1)治理域：包含五个治理流程，在每个流程中都定义了评价、指导、监督(EDM)实践

(2)管理域：包含四个符合计划、建立、运行、监测(PBRM)的职能域

图31-COBIT 5流程参照模型



5、名称定义变化：

（1）COBIT5 治理或管理实践等同于 COBIT4.1 控制目标和 VAL IT 及 RISK IT 流程。

例如：实践即如 BAI10-管理配置、DSS03-管理问题

（2）COBIT5 活动等同于 COBIT4.1 控制实践和 VAL IT 及 RISK IT 管理实践

例如：活动即如 BAI10.01-建立和维护配置模型

（六）、RACI 图更明细

1、COBIT4.1 的 RACI 图

RACI 图 职能

活动	董事执行官	董事财务官	业务执行经理	董事信息官	业务流程所有者	运营总监	董事架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
建立业务目标和 IT 目标间的关联	C	I	A/R	R	C						
识别关键依赖和当前绩效	C	C	R	A/R	C	C	C	C	C		C
建立 IT 战略规划	A	C	C	R	I	C	C	C	C	I	C
建立 IT 战术计划	C	I		A	C	C	C	C	C	R	I
分析项目群投资组合，并管理项目和服务的投资组合	C	I	I	A	R	R	C	R	C	C	I

RACI 图中，Responsible 代表**执行**，Accountable 代表**负责**，Consulted 代表**商议**，Informed 代表**告知**。

2、COBIT5 的 RACI 图

（1）COBIT5 采用与 COBIT4.1、Val IT 和 Risk IT 类似的方法描述角色和职责

（2）COBIT5 提供了一个比 COBIT4.1 更为完整、明确和清晰的通用业务和 IT 参与者的范围，从而在规划和实施流程时能更好地定义角色参与者的职责或参与的程度。

BAI10 RACI表																								
关键管理实践	董事会	首席执行官	首席财务官	首席运营官	业务主管	业务流程所有者	战略执行委员会	指导委员会(方案、项目)	项目管理办公室	价值管理办公室	首席风险官	首席信息安全官	架构委员会	企业风险委员会	人力资源主管	合规部	审计部	首席信息官	架构主管	开发主管	IT运营主管	IT管理主管	服务经理	信息安全经理	业务持续性经理	隐私主官
BAI10.01 配置和维护配置模型						C											C	C	C	I	A	R	R			
BAI10.02 建立和维护配置库和基线																			C	R	A	R	R			
BAI10.03 维护和控制配置项																		A	C	R	R	R	C			
BAI10.04 生成状态和配置报告						I											I	I	C	C	A	R	I			
BAI10.05 验证和审查配置库的完整性						I											R		R	R	A		R			

（七）、控制流程描述更清晰

1、COBIT5 控制流程

（1）COBIT5 流程提供了更全面和完全覆盖反映普遍企业 IT 使用特性的做法。它使运用 IT 的利益相关者的参与、责任和职责更明确和透明。

（2）COBIT5 整合和更新了所有先前的内容到一个新模型，使用户在实施改进时更易于理解和使用这些资料

（3）按照以下思路进行流程描述：流程识别、流程目的表述，流程目标级联信息，流程目标和度量指标，RACI 表，流程实践（含子流程）、输入输出和流程实施活动、相关参照指南等

（4）更多控制流程信息参阅汇哲 COBIT5.0 Processs 中文版

2、COBIT4.1 控制流程

(1)按照以下思路进行流程描述：流程的主要内容和目标、对应流程所包含的详细控制目标、流程输入和输出、RACI 图、目标和衡量指标、流程的成熟度模型

3、流程描述的输入和输出

COBIT5 对每一个管理实践(活动)提供了输入输出，而 COBIT4.1 只在流程层级提供。

4、流程控制活动更完整

（八）、更新了流程成熟度模型

1、COBIT5 中止了 COBIT4.1、 Val IT 和 Risk IT 基于 CMM 能力成熟度模型方法。
2、COBIT5 借鉴了 ISO/IEC 15504 成熟度模型，重新对成熟度级别进行了定义，基于 ISO/IEC 15504 建立新的流程能力评估方法，而且建立了替代 COBIT4.1 中 CMM 方法的 COBIT 评估程序。
3、COBIT 评估程序方法是 ISACA 组织认为更强健、更可靠和可重复的流程能力评估方法。
4、COBIT 评估程序支持：
(1)认可评审顾问的正式评估(评审顾问培训正在开发中)
(2)减少对内部差距分析和流程改进计划严格的自评估
5、将来，COBIT 评估程序也极可能使企业获得符合 ISO/IEC 标准规范的独立自主的和认证评估。
6、更新和对照了成熟度模型的通用属性

图 21－成熟度属性(COBIT4.1)和流程属性(COBIT 5)对照表									
COBIT4.1 成熟度属性	COBIT 5 能力属性								
	流程执行	绩效管理	工作成果管理	流程定义	流程部署	流程管理	流程控制	流程创新	流程优化
意识和沟通				■	■	■			
政策、计划和实施程序							■		
工具和自动化方案				■					
技能和专业经验				■	■				
职责和责任				■					
目标设定和衡量		■				■			

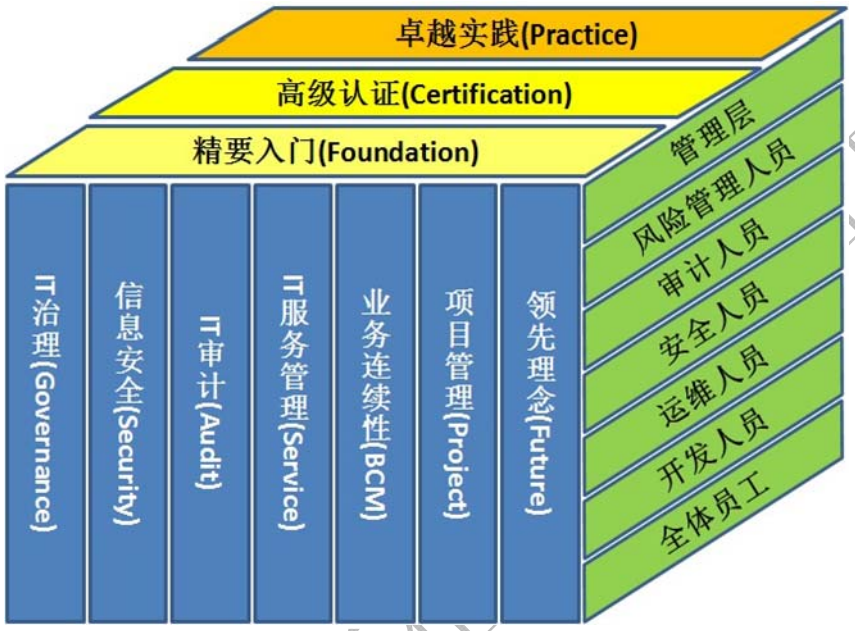
（九）、IT 信息准则比照

COBIT5 与 COBIT4.1 相等的信息标准	
COBIT4.1 信息标准	**COBIT 5** 相等的信息质量目标
效果(有效性,Effectiveness)	适量的，相关性，可理解性，解释性，客观性
效率(Efficency)	可信度，可访问性，易于操作，信誉度。
完整性(Integrity)	完全性，准确性
可靠性(Reliability)	可信度，信誉度，客观性
可用性(Availablity)	可用性是信息的质量目标之一，处于可访问性和安全性栏目下。
保密性(Confidentiality)	保密性对应“限制访问”的信息质量目标
合规性(Compliance)	合规性涵盖在所有的信息质量目标中。

COBIT5 也允许设置另外的信息标准。

三、 汇哲最新课程体系：

汇哲培训服务三维体系，360 度覆盖您的培训需求！



详细请联系：

上海总部
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：huizhe@spisec.com

北京分部：
电话：010-56193081
地址：北京市上地十街辉煌国际广场 5 号楼 713
邮编：100085
邮箱：huizhebj@spisec.com

广西分部：
电话：0771—2875867
地址：广西南宁兴宁区民生路 131 号绿都商厦 1001
邮编：530012
邮箱：huizhegx@spisec.com