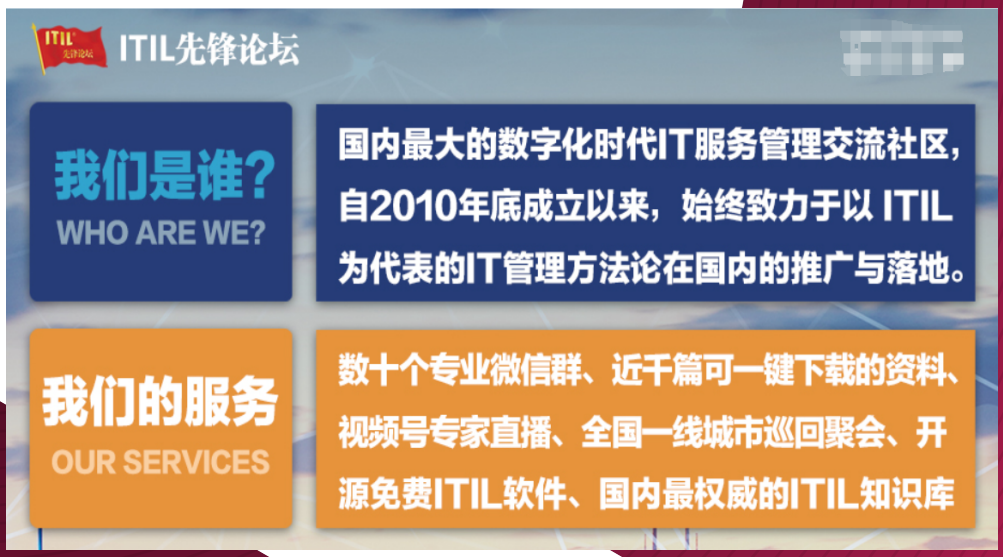
COBIT 2019

框架

治理和管理目标



ISACA

目录

第 1 章. COBIT® 2019 简介 9
1.1 COBIT 是信息和技术治理框架 9
1.1.1 COBIT 是什么？不是什么？ 9
1.2 COBIT® 2019 概述 10
1.3 COBIT 框架的术语和关键概念 11
1.3.1 治理和管理目标 11
1.3.2 治理系统的组件 12
1.3.3 焦点领域 14

第 2 章. 本出版物的结构和目标受众 15
2.1 本出版物的结构 15
2.2 目标受众 15

第 3 章. COBIT 治理和管理目标的结构 17
3.1 简介 17
3.2 治理和管理目标 17
3.3 目标级联 18
3.4 组件：流程 19
3.5 组件：组织结构 20
3.6 组件：信息流和信息项 22
3.7 组件：人员、技能和胜任能力 24
3.8 组件：政策和程序 25
3.9 组件：文化、道德和行为 25
3.10 组件：服务、基础设施和应用程序 25

第 4 章. COBIT 治理和管理目标 – 详细指南 27
COBIT 核心模型 27
4.1 评估、指导和监控 (EDM) 27
4.2 调整、规划和组织 (APO) 53
4.3 内部构建、外部采购和实施 (BAI) 151
4.4 交付、服务和支持 (DSS) 229
4.5 监控、评价和评估 (MEA) 271

附录 297
5.1 附录 A：目标级联 — 对应关系表 297
5.2 附录 B：组织结构 — 概述和描述 299
5.3 附录 C：参考资料详细清单 300

图表列表

第 1 章. COBIT® 2019 简介

图 1.1 — COBIT 概述....10
图 1.2 — COBIT 核心模型....12
图 1.3 — COBIT 治理系统的组件....13

第 3 章. COBIT 治理和管理目标的结构

图 3.1 — 治理和管理目标展示....18
图 3.2 — 适用的企业目标和一致性目标展示....18
图 3.3 — 适用的目标和指标示例展示....19
图 3.4 — 流程组件展示....19
图 3.5 — 流程的能力级别....20
图 3.6 — 组织结构组件展示....21
图 3.7 — 信息流和信息项组件展示....23
图 3.8 — 到多个流程的输出....23
图 3.9 — 人员、技能和胜任能力组件展示....24
图 3.10 — 政策和程序组件展示....25
图 3.11 — 文化、道德和行为组件展示....25
图 3.12 — 服务、基础设施和应用程序组件展示....25

附录

图 5.1 — 企业目标与一致性目标的对应关系....297
图 5.2 — 治理和管理目标与一致性目标的对应关系....298
图 5.3 — COBIT 角色和组织结构....299

第 1 章
COBIT® 2019 简介

1.1 COBIT 是信息和技术治理框架

近年来，业界开发和推广了多种最佳实践框架，来协助完成企业 IT 治理 (EGIT) 的理解、设计和实施过程。COBIT® 2019 集该领域内超过 25 年的开发成果之大成，不仅融入了新的科学见解，还将这些见解付诸于实践。

COBIT® 立足 IT 审计领域，如今已发展为一种更广泛、更全面的信息和技术 (I&T) 治理和管理框架，进而确立了其面向 I&T 治理的行业公认框架的地位。

1.1.1 COBIT 是什么？不是什么？

在介绍更新的 COBIT 框架之前，有必要解释一下 COBIT 是什么和不是什么：

COBIT 是面向整个企业的信息和技术治理及管理框架。企业 I&T 是指企业为实现其目标而在任何领域实施的所有技术和信息处理。换句话说，企业 I&T 包括但不仅限于组织的 IT 部门。

COBIT 框架对治理和管理进行了明确区分。这两个学科涵盖不同的活动，需要不同的组织结构，并服务于不同目的。

- **治理**确保：
  - 对利益相关方的需求、条件和选择方案进行评估，以确定全面均衡、达成共识的企业目标。
  - 通过确定优先等级和制定决策来设定方向。
  - 根据议定的方向和目标监控绩效与合规性。

  在大多数企业中，治理是董事长领导下的董事会的职责。具体的治理职责可以赋予合适级别的专门组织结构，特别是在大型的复杂企业中。
- **管理**是指按治理机构设定的方向计划、构建、运行和监控活动，以实现企业目标。

  在大多数企业中，管理是首席执行官 (CEO) 领导下的高级管理层的职责。

COBIT 定义了构建和维持治理系统的组件：流程、组织结构、政策和程序、信息流、文化和行为、技能以及基础设施。[1]

COBIT 阐明了企业应考虑的设计因素，以建立最合适的治理系统。

COBIT 在解决治理问题时采用的方法是，将相关的治理组件归类为可在所需的能力级别进行管理的治理和管理目标。

[1] 在 COBIT® 5 中，这些组件被称为“动力”。

关于 COBIT 有一些误解需要澄清：

- COBIT 不是整个企业 IT 环境的完整说明。
- COBIT 不是用于组织业务流程的框架。
- COBIT 不是用于管理所有技术的 IT 技术框架。
- COBIT 不做出或规定任何 IT 相关的决策。它的目的不是确定最佳 IT 战略是什么、最佳架构是什么以及可能或应该投入多少 IT 成本，而是定义旨在描述应做出何种决策以及如何和由谁做出决策的所有组件。

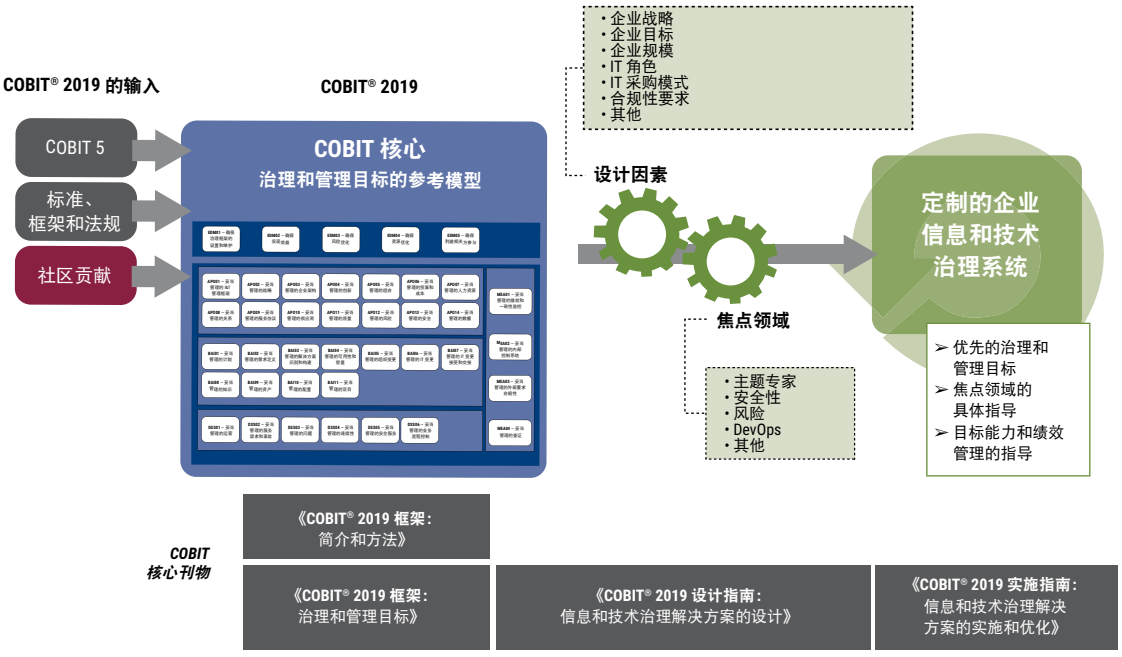
1.2 COBIT® 2019 概述

COBIT® 2019 产品系列是采用可定制设计的开放式框架。目前提供以下出版物。[2]

- ***《COBIT® 2019 框架：简介和方法》***介绍了 COBIT® 2019 的关键概念。
- ***《COBIT® 2019 框架：治理和管理目标》***全面介绍了 40 项核心治理和管理目标，以及其中包含的流程和其他相关组件。本指南还参考了其他标准和框架。
- ***《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》***探讨了可能影响治理的设计因素，并包含了规划定制的企业治理系统的工作流程。
- ***《COBIT® 2019 实施指南：信息和技术治理解决方案的实施和优化》***是*《COBIT® 5 实施指南》*的演进版，并制定了一份持续改进治理的路线图。它可以和*《COBIT® 2019 设计指南》*结合使用。

图 1.1 高度概括了 COBIT® 2019，说明了该系列不同出版物所涵盖的不同方面。

图 1.1 — COBIT 概述



[2] 本*《COBIT® 2019 框架：治理和管理目标》*出版时，COBIT® 2019 产品系列的其他书刊也已纳入计划，但尚未发布。

图 1.1 中标识为焦点领域的内容将包含有关特定主题的更详细指导。[3]

未来，COBIT 将呼吁用户社区提供内容更新建议并持续采纳和管理这些建议，使 COBIT 与最新的行业见解和发展保持同步。

以下章节介绍 COBIT® 2019 中使用的关键概念和术语。

1.3 COBIT 框架的术语和关键概念

1.3.1 治理和管理目标

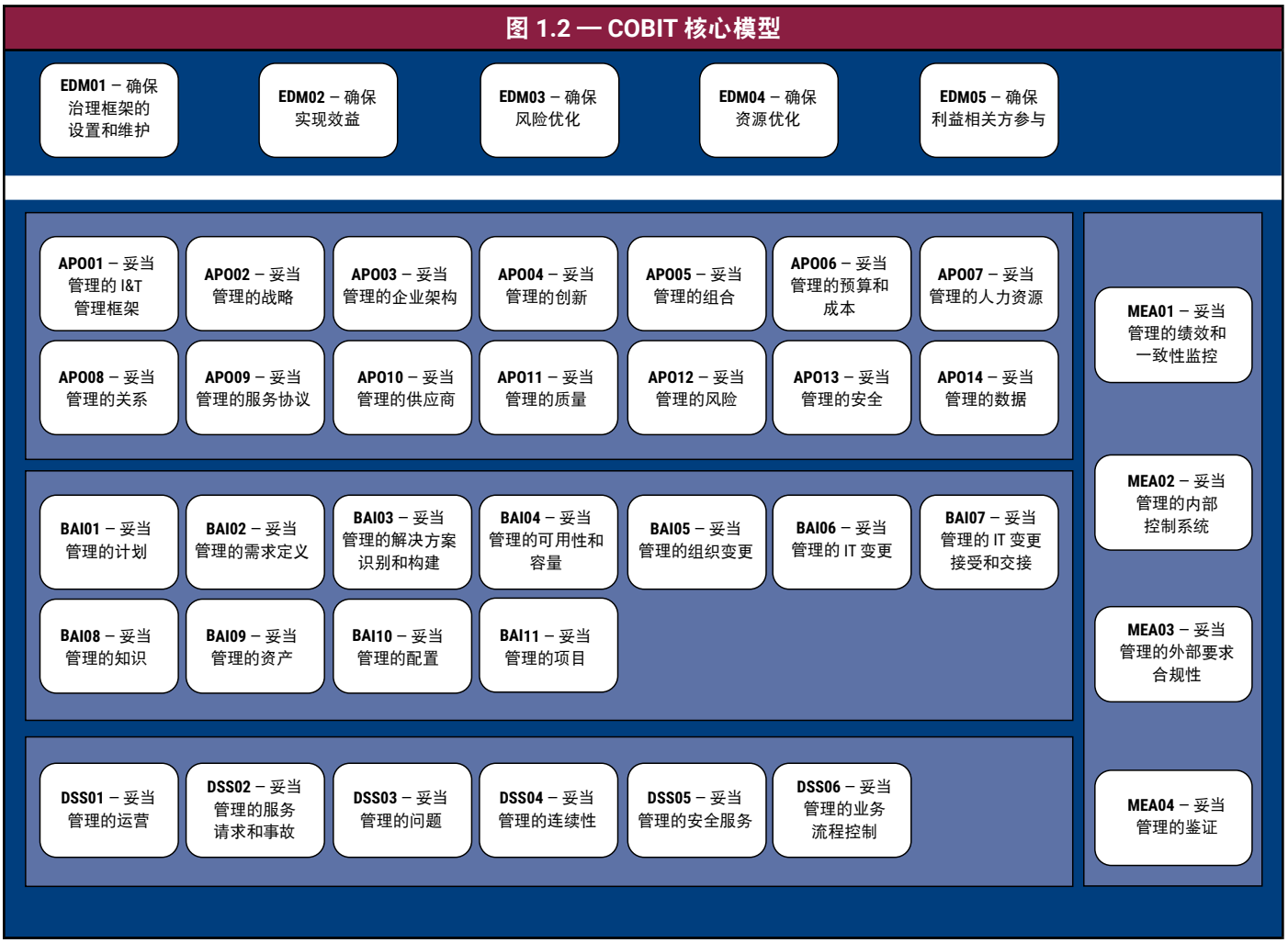
要让信息和技术促进企业目标的实现，应达成一系列的治理和管理目标。有关治理和管理目标的基本概念包括：

- 治理或管理目标**总会涉及一个流程**（具有相同或相似的名称）和一系列其他类型的相关组件，以帮助实现目标。
- 治理目标与治理流程（如**图 1.2** 中深蓝色背景所示）有关，而管理目标与管理流程（如**图 1.2** 中浅蓝色背景所示）有关。治理流程通常由董事会和执行管理层负责，而管理流程则在高级和中级管理层的职责范围内。

COBIT 中的治理和管理目标分为五个领域。这些领域的名称包含动词，传达了主要目的及目标涵盖的活动领域：

- 治理目标被列入**评估、指导和监控** (EDM) 领域。在这个领域，治理机构将评估战略方案、指导高级管理层执行所选的战略方案并监督战略的实施。
- 管理目标分为四个领域：
  - **调整、规划和组织** (APO) 针对 I&T 的整体组织、战略和支持活动。
  - **内部构建、外部采购和实施** (BAI) 针对 I&T 解决方案的定义、采购和实施以及它们到业务流程的整合。
  - **交付、服务和支持** (DSS) 针对 I&T 服务的运营交付和支持，包括安全。
  - **监控、评价和评估** (MEA) 针对 I&T 的性能监控及其与内部性能目标、内部控制目标和外部要求的一致程度。

[3] 目前正在准备其中多个焦点领域的内容指南，其余焦点领域也已纳入计划。这些焦点领域的指南是开放式的，将会不断完善。有关目前已发布和计划发布的出版物的最新信息和其他内容，请访问 *www.isaca.org/cobit*。



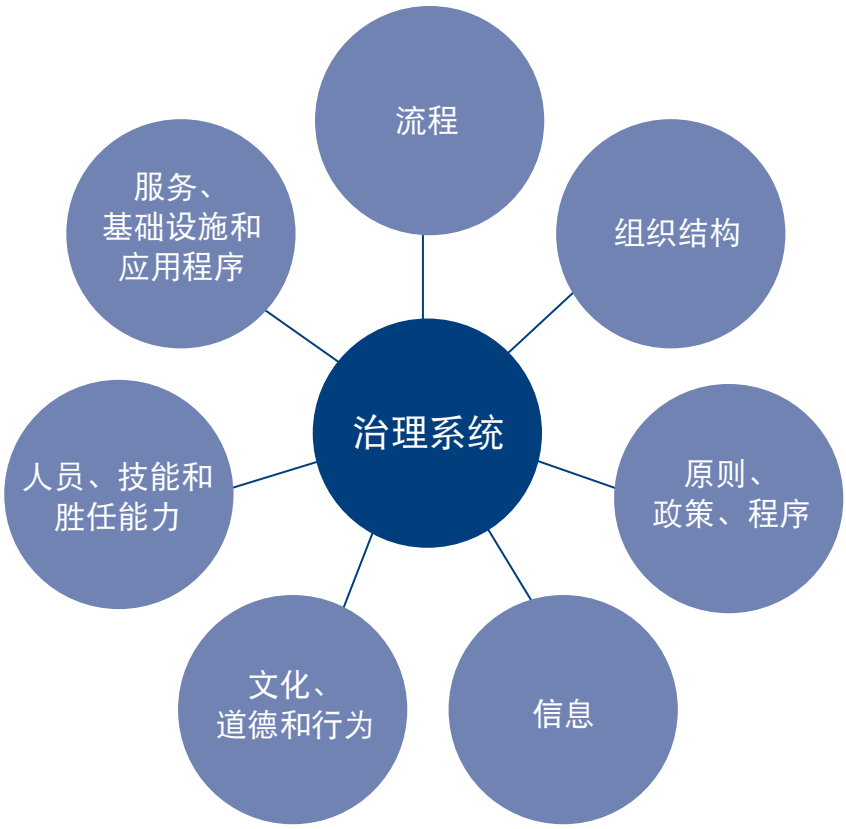
1.3.2 治理系统的组件

为满足治理和管理目标，每个企业都需要建立、定制和维护由多个组件构成的治理系统。

- 组件是单独或共同促进企业的 I&T 治理系统良好运营的因素。
- 组件彼此交互，形成了一个整体性的 I&T 治理系统。
- 组件可以是不同类型的。最熟悉的组件是流程。治理系统的组件也包括组织结构、政策和程序、信息项目、文化和行为、技能和能力以及服务、基础设施和应用程序（**图 1.3**）。
  - **流程**描述了一组为实现某种目标而安排有序的实践和活动，并生成了一组支持实现整体 IT 相关目标的输出内容。
  - **组织结构**是企业的主要决策实体。
  - **原则、政策和框架**用于将理想行为转化为日常管理的实用指南。
  - 在任何组织中，**信息**无处不在，包括企业生成和使用的全部信息。COBIT 侧重于有效运转企业治理系统所需的信息。

- 个人和企业的**文化、道德和行为**作为治理和管理活动的成功因素，其价值往往被低估。
- **人员、技能和胜任能力**对做出正确决策、采取纠正行动和成功完成所有活动而言是必不可少的。
- **服务、基础设施和应用程序**包括为企业提供 I&T 处理治理系统的基础设施、技术和应用程序。

图 1.3 — COBIT 治理系统的组件



所有类型的组件都可能是通用的，也可能是通用组件的变体：

- **通用**组件在 COBIT 核心模型（请参阅**图 1.2**）中描述，原则上可以应用于任何情况。但是，它们本质上虽是通用的，在实际实施之前却通常需要定制。
- **变体**组件基于通用组件，但针对特定目的或焦点领域内的环境（如信息安全、DevOps 或特定法规）进行了定制。

1.3.3 焦点领域

焦点领域描述了一个特定的治理主题、领域或问题，可以通过一系列治理和管理目标及其组件来解决。焦点领域的例子包括：中小型企业、网络安全、数字化转型、云计算、隐私和 DevOps。[4]

COBIT 核心模型是本出版物的主题，它提供了通用的治理组件。焦点领域可能同时包含通用治理组件以及为该焦点领域主题定制的特定组件变体。

焦点领域的数量几乎没有限制，正因如此，COBIT 是开放式的。可根据需要添加新的焦点领域，或由主题专家和从业人员对开放式 COBIT 模型进行添加。

多个焦点领域的内容指南正在准备中，该系列将不断完善。有关目前已发布和计划发布的出版物的最新信息和其他内容，请访问 *www.isaca.org/cobit*。

[4] DevOps 是组件变体和焦点领域的例证。为什么？DevOps 是市场中的最新主题，而且非常需要具体指导，因而成为一个焦点领域。DevOps 包括核心 COBIT 模型的若干通用治理和管理目标，以及与开发、运营和监控相关的流程及组织结构的一系列变体。

第 2 章
本出版物的结构和目标受众

2.1 本出版物的结构

本出版物全面介绍了 COBIT 核心模型（**图 1.2**）中定义的 40 项核心治理和管理目标，以及其中包含的流程、其他相关组件和相关指南的参考资料，如其他标准和框架。附录 C 中提供了所含参考资料来源的详细清单。

本文档其余部分包含下列章节和附录：

- 第 3 章所介绍的结构用于详细导览跨组件的 40 项治理和管理目标。
- 第 4 章全面介绍了 COBIT 核心模型（**图 1.2**）中定义的 40 项核心治理和管理目标，以及其中包含的流程、其他相关组件和相关指南参考资料，如其他标准和框架。
- 附录中包含以下方面的更多详细信息：
  - 显示目标级联的对应关系表
  - 组织结构的描述
  - 参考资料来源清单

2.2 目标受众

本指南的目标受众是整个企业内的各类专业人员，包括业务、审计、安全、风险管理、IT 和其他从业者，他们将从有关 COBIT 核心模型的 40 项治理和管理目标的详细指南中受益。若要定制 COBIT 以形成有针对性的企业治理实践，需要一定的经验水平并对企业有一定的了解。

第 3 章
COBIT 治理和管理目标的结构

3.1 简介

本章介绍了用于详述各项 COBIT 治理和管理目标的结构。针对每项治理和管理目标，本出版物的第 4 章提供了适用于该目标的各个**治理组件**的相关信息：

- 流程
- 组织结构
- 信息流和信息项
- 人员、技能和胜任能力
- 政策和程序
- 文化、道德和行为
- 服务、基础设施和应用程序

这些信息的结构将在下面的章节中详细介绍。

3.2 治理和管理目标

如前所述，COBIT® 2019 包含 40 项治理和管理目标，分为五个领域（请参阅**图 1.2**）。

- **治理**领域
  - 评估、指导和监控 (EDM)
- **管理**领域
  - 调整、规划和组织 (APO)
  - 内部构建、外部采购和实施 (BAI)
  - 交付、服务和支持 (DSS)
  - 监控、评价和评估 (MEA)

对于每项目标，详述的高级别信息（**图 3.1**）包括：

- 领域名称
- 焦点领域（在本出版物中为 COBIT 核心模型）
- 治理或管理目标名称
- 描述
- 目的说明

图 3.1 — 治理和管理目标展示	
领域：<名称> **治理/管理目标：**<名称>	**焦点领域：**<名称>
描述	
<文本>	
目的	
<文本>	

3.3 目标级联

每项治理或管理目标都支持实现与更大的企业目标相关的一致性目标（请参阅《*COBIT® 2019 框架：简介和方法*》的第 4.6 节了解更多信息，并参阅附录 A 中目标级联对应关系表中的示例）。

与当前治理或管理目标存在主要关联的一致性目标列在该目标详细指南的右侧部分（**图 3.2**）。

图 3.2 — 适用的企业目标和一致性目标展示		
治理/管理目标支持实现一系列主要企业目标和一致性目标：		
企业目标	➡	**一致性目标**
• <EG 编号> <目标描述>		• <AG 编号> <目标描述>

一致性目标包括：

- AG01：I&T 合规且支持业务部门遵守外部法律和法规
- AG02：妥善管理的 I&T 相关风险
- AG03：通过 I&T 促成的投资和服务组合所实现的效益
- AG04：技术相关财务信息的质量
- AG05：提供符合业务需求的 I&T 服务
- AG06：将业务需求转化为可运作的解决方案的敏捷性
- AG07：信息、参与执行的基础设施和应用程序的安全，以及隐私的安全
- AG08：通过集成应用程序和技术来推行和支持业务流程
- AG09：在预算内按时交付计划且满足要求和质量标准
- AG10：I&T 管理信息的质量
- AG11：I&T 遵守内部政策
- AG12：既了解技术又熟知业务、能力出众且积极上进的员工
- AG13：业务创新的知识、专业技能和举措

与所列一致性目标存在主要关联的企业目标显示在相应目标详细指南（第 4 章）的左侧部分。企业目标包括：

- EG01：有竞争力的产品和服务的组合
- EG02：妥当管理的业务风险

- EG03：遵守外部法律和法规
- EG04：财务信息的质量
- EG05：以客户为中心的服务文化
- EG06：业务服务连续性和可用性
- EG07：管理信息的质量
- EG08：业务流程功能的优化
- EG09：业务流程成本的优化
- EG10：员工技能、动力和生产力
- EG11：遵守内部政策
- EG12：妥当管理的数字化转型计划
- EG13：产品和业务创新

表中还提供了企业目标和一致性目标的指标示例（**图 3.3**）。

图 3.3 — 适用的目标和指标示例展示

治理/管理目标支持实现一系列主要企业目标和一致性目标：		
企业目标	→	**一致性目标**
<EG 编号> <目标描述>		<AG 编号> <目标描述>
企业目标的指标示例		**一致性目标的指标示例**
<EG 编号> •<指标>		<AG 编号> •<指标>
<EG 编号> •<指标>		<AG 编号> •<指标>

3.4 组件：流程

每项治理和管理目标包含多个流程实践。每个流程包含一项或多项活动。每个流程实践包含若干配套指标示例，用于衡量实践的成果及其对于实现总体目标的贡献（**图 3.4**）。

图 3.4 — 流程组件展示

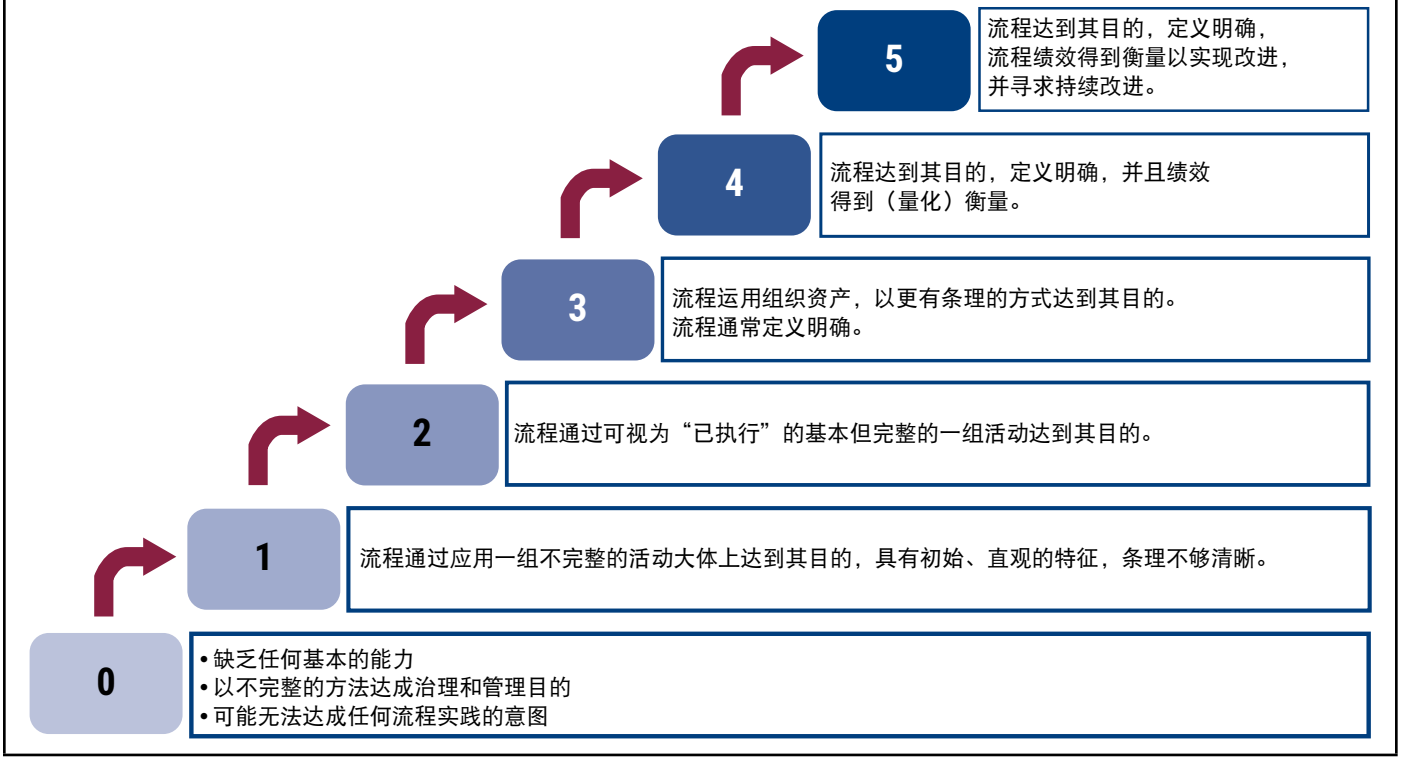
A. 组件：流程	
治理/管理实践	**指标示例**
<编号> <名称> <描述>	<指标>

活动	**能力级别**
1. <文本>	<NR>
2. <文本>	<NR>
n. <文本>	<NR>

相关指南（标准、框架、合规性要求）	**详细参考**
<标准名称>	<文本>
<标准名称>	<文本>

所有流程活动都会分配能力级别，帮助明确定义处在不同能力级别的流程。成功完成特定能力级别的所有活动后，即表明流程达到了相应的能力级别。COBIT® 2019 支持基于能力成熟度模型集成 (CMMI®) 的流程能力方案，范围为 0 到 5 级。能力级别用于衡量流程的实施和执行情况。**图 3.5** 描述了模型、递增的能力级别以及每个级别的一般特征。

图 3.5 — 流程的能力级别



请参阅《*COBIT® 2019 框架：简介和方法*》的第 6 章，了解有关绩效管理和能力衡量的更多详细信息。

适用情况下，此部分还会包含其他标准和指南的参考信息（请参阅**图 3.4**）。相关指南是指与当前流程相关的所有标准、框架、合规性要求和其他指南。详细参考部分会引用相关指南中的具体章节。附录 C 中提供了完整的相关指南来源清单。

如果某个特定组件没有列出相关指南，则表示对应来源中没有已知的适用参考内容。欢迎广大从业者提出相关指南建议。

3.5 组件：组织结构

组织结构治理组件提供了关于流程实践的职责和责任级别的建议（**图 3.6**）。图表中包含了业务和 IT 部门的单独角色及组织结构。

图 3.6 — 组织结构组件展示								
B. 组件：组织结构								
关键治理/管理实践	**组织结构 1**	**组织结构 2**	**组织结构 3**	**组织结构 4**	**组织结构 5**	**组织结构 6**	**组织结构 7**	**组织结构 8，等等**
<编号><名称>								

相关指南（标准、框架、合规性要求）	详细参考
<标准名称>	<文本>
<标准名称>	<文本>

在 COBIT® 2019 的相关资料中定义了下列角色和组织结构：

- 董事会
- 执行委员会
- 首席执行官
- 首席财务官
- 首席运营官
- 首席风险官
- 首席信息官
- 首席技术官
- 首席数字官
- I&T 治理委员会
- 架构委员会
- 企业风险委员会
- 首席信息安全官
- 业务流程所有者
- 组合经理
- （计划/项目）指导委员会
- 计划经理
- 项目经理
- 项目管理办公室
- 数据管理部门
- 人力资源总监
- 关系经理

- 架构总监
- 开发总监
- IT 运营总监
- IT 行政总监
- 服务经理
- 信息安全经理
- 业务连续性经理
- 隐私官
- 法律顾问
- 合规官
- 审计

附录 B 中提供了其中每个角色和组织结构的详细描述。这些结构包含的不同参与级别可分为负责人级别和责任人级别。

- **负责人** (R) 角色在执行实践方面承担主要运营职责，并负责实现预期成果。由谁来完成任务？由谁来推动任务的进展？
- **责任人** (A) 角色承担总体责任。原则上责任不能分担。由谁负责确保成功完成任务并取得成果？

每个领域都描述了在该领域承担职责和/或责任的组织机构。图表中提供了每个角色和组织结构的详细描述。其他未承担职责或责任的组织机构已被省略，以方便阅读。

从业者可通过为角色和组织结构添加这两个参与级别来完善图表。由于咨询人和被通知人角色的归属取决于组织环境和优先级，因此本详细指南中未包括这些角色。

- **咨询人** (C) 角色为实践提供建议。由谁提供建议？
- **被通知人** (I) 角色须获知实践的成果和/或交付成果。谁将收到信息？

企业应该审查职责和责任级别、咨询人和被通知人，并根据企业的环境、优先级和首选术语来更新图表中的角色和组织结构。

适用情况下，组织结构组件部分将会提供其他标准和更多指南的参考信息。相关指南是指与当前组织结构及其流程参与级别相关的所有标准、框架、合规性要求和其他指南。详细参考部分会引用相关指南中的具体章节。附录 C 中提供了完整的来源清单。

3.6 组件：信息流和信息项

第三个治理组件提供了与流程实践相关联的信息流和信息项的指南。每个实践包含输入和输出，并指出了来源和目标。

一般而言，每项输出会被发送到一个或若干个目标（通常是其他 COBIT 流程实践）。然后该输出将成为其目标的输入（**图 3.7**）。

图 3.7 — 信息流和信息项组件展示				
C. 组件：信息流和信息项				
治理/管理实践	输入		输出	
<编号> <名称>	自	描述	描述	至
	<编号>	<文本>	<文本>	<编号>

相关指南（标准、框架、合规性要求）	详细参考
<标准名称>	<文本>
<标准名称>	<文本>

不过，有些输出具有多个目标，例如所有 COBIT 流程或某个领域内的所有流程。出于可读性的原因，没有将这些输出列为目标流程的输入。**图 3.8** 提供了此类输出的完整列表。

对于某些输入/输出，如果输入和输出是在同一流程的不同活动之间共享，则会以“内部”作为目标。

图 3.8 — 到多个流程的输出		
到所有流程的输出		
来自关键实践	输出描述	目标
APO13.02	信息安全风险处置计划	所有 EDM，所有 APO；所有 BAI；所有 DSS；所有 MEA
来自治理实践	输出描述	目标
EDM01.01	企业治理指导原则	所有 EDM
EDM01.01	决策模式	所有 EDM
EDM01.02	企业治理沟通	所有 EDM
EDM01.01	权限级别	所有 EDM
EDM01.03	关于治理有效性和绩效的反馈	所有 EDM
到所有管理流程的输出		
来自管理实践	输出描述	目标
APO01.01	管理系统设计	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO01.01	优先的治理和管理目标	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO01.02	关于 I&T 目标的沟通	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO01.02	沟通的基本原则	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO01.03	目标模型差距分析	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO01.11	流程改进机会	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO02.05	I&T 战略和目标	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO02.06	沟通工作包	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO11.03	质量管理标准	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO11.04	流程服务质量目标和指标	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO11.05	关于持续改进和最佳实践的沟通	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO11.05	需要分享的良好实践示例	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO11.05	质量审查基准指标结果	所有 APO；所有 BAI；所有 DSS；所有 MEA

图 3.8 — 到多个流程的输出（续）		
到所有管理流程的输出		
来自管理实践	输出描述	目标
MEA01.02	监控目标	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA01.04	绩效报告	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA01.05	补救措施和工作分配	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA02.01	内部控制的监控和审查结果	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA02.01	基准检测和其他评估的结果	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA02.03	自我评估审查的结果	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA02.03	自我评估计划和衡量标准	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA02.04	控制缺陷	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA02.04	补救措施	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA03.02	合规要求变更的沟通	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA04.02	鉴证计划	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA04.08	鉴证审查报告	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA04.08	鉴证审查结果	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA04.09	补救措施	所有 APO；所有 BAI；所有 DSS；所有 MEA

适用情况下，信息流和信息项组件将会提供其他标准和更多指南的参考信息。相关指南是指与当前信息项目相关的所有标准、框架、合规性要求和其他指南。详细参考部分会引用相关指南中的具体章节。附录 C 中提供了完整的来源清单。

3.7 组件：人员、技能和胜任能力

人员、技能和胜任能力治理组件指定实现治理或管理目标所需的人力资源和技能。COBIT® 2019 为本指南提供了信息时代的技能框架 (SFIA®) V6（第 6 版）[5] 作为基础。SFIA 框架中详细介绍了所有列出的技能。“详细参考”部分提供了对应该技能的 SFIA 指南的唯一代码（**图 3.9**）。此外，针对若干治理和管理目标，还提供了以下参考资料：*《e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework*[6]》和内部审计师学会的 “Core Principles for the Professional Practice of Internal Auditing”。[7]

图 3.9 — 人员、技能和胜任能力组件展示		
D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
<名称>	信息时代的技能框架，第 6 版 (SFIA 6)，2015 年	<SFIA 代码>
<名称>	信息时代的技能框架，第 6 版 (SFIA 6)，2015 年	<SFIA 代码>

[5] SFIA Foundation，“SFIA V6, the sixth major version of the Skills Framework for the Information Age.”，*https://www.sfia-online.org/en/framework/sfia-6*
[6] 欧洲标准化委员会 (CEN)，e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，EN 16234-1:2016，*https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT:41798&cs=13E00999DD92E702F0E171397CF76EC87*
[7] 内部审计师学会® (IIA®)，“Core Principles for the Professional Practice of Internal Auditing”，*https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Core-Principles-for-the-Professional-Practice-of-Internal-Auditing.aspx*

3.8 组件：政策和程序

此组件提供治理或管理目标的相关政策和程序的详细指南。其中包含相关政策和程序的名称，以及政策目的和内容的描述（**图 3.10**）。

适用情况下，还会提供其他标准和更多指南的参考信息。“相关指南”部分引用了相关指南中的具体章节，可参考这些章节获取更多信息。附录 C 中提供了完整的来源清单。

图 3.10 — 政策和程序组件展示

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
<名称>	<描述>	<标准名称>	<文本>

3.9 组件：文化、道德和行为

文化、道德和行为治理组件提供关于组织内支持实现治理或管理目标所需的文化元素的详细指南（**图 3.11**）。适用情况下，还会提供其他标准和更多指南的参考信息。“相关指南”部分引用了相关指南中的具体章节，可参考这些章节获取更多信息。附录 C 中提供了完整的来源清单。

图 3.11 — 文化、道德和行为展示

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
<名称>	<标准名称>	<文本>

3.10 组件：服务、基础设施和应用程序

服务、基础设施和应用程序治理组件提供关于可用于支持实现治理或管理目标的第三方服务、基础设施类型和应用程序类别的详细指南。指南是通用的（以避免指定具体的供应商或产品名称）；但条目内容仍然为企业构建自己的 I&T 治理系统提供了指导（**图 3.12**）。

图 3.12 — 服务、基础设施和应用程序组件展示

G. 组件：服务、基础设施和应用程序
<服务、基础设施或应用程序类别>

第 4 章
COBIT 治理和管理目标 — 详细指南

COBIT 核心模型

4.1 评估、指导和监控 (EDM)

01 确保治理框架的设置和维护

02 确保实现效益

03 确保风险优化

04 确保资源优化

05 确保利益相关方参与

领域：评估、指导和监控 治理目标：EDM01 — 确保治理框架的设置和维护	焦点领域：COBIT 核心模型

描述

分析和阐明企业 I&T 治理要求。落实和维护治理组件，明确权限和职责，以实现企业的使命、目的和目标。

目的

提供与企业治理方法相结合的一致方法，I&T 相关决策应该与企业的战略和目标保持一致，并实现期望的价值。为此，应确保 I&T 相关流程得到有效和透明的监督，符合法律、合同和监管要求，以及满足董事会成员的治理要求。

治理目标支持一系列主要企业目标和一致性目标的实现：

企业目标	一致性目标
• EG03 遵守外部法律和法规 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	• AG01 I&T 合规且支持业务部门遵守外部法律和法规 • AG03 通过 I&T 促成的投资和服务组合所实现的效益

企业目标的指标示例		一致性目标的指标示例	
EG03	a. 不合规的成本，包括结算和罚款 b. 引起负面舆论或负面影响的不合规问题的数量 c. 监管机构指出的违规问题的数量 d. 与业务伙伴合同协议有关的不合规问题的数量	AG01	a. IT 不合规的成本，包括费用结算和罚款，以及声誉损失造成的影响 b. 向董事会报告或者引起舆论或难堪的 IT 相关不合规问题的数量 c. 与 IT 服务提供商的合同协议有关的不合规问题的数量
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度	AG03	a. 达到或超过业务案例宣称效益的 I&T 促成的投资的百分比 b. 实现预期效益（如服务水平协议所述）的 I&T 服务的百分比
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比		

A. 组件：流程

治理实践	指标示例
EDM01.01 评估治理系统。 持续识别企业的利益相关方并与其沟通，记录对需求的理解，并评估当前和未来的企业 I&T 治理设计。	a. 为 I&T 治理和决策定义的指导原则的数量 b. 参与设定 I&T 治理方向的高级管理人员的数量

活动	能力级别
1. 分析并确定可能影响治理设计的内部和外部环境因素（法律、法规和合同义务）以及商业环境中的趋势。	2
2. 确定 I&T 的重要性及其相对于业务的角色。	
3. 考虑外部法规、法律和合同义务，并确定如何将其应用于企业 I&T 治理。	
4. 确定总体企业控制环境在 I&T 方面的影响。	
5. 使信息的合理使用和处理及其对社会、自然环境和内外部利益相关方利益的影响与企业的方向、目的和目标保持一致。	3
6. 阐明指导 I&T 治理设计和决策制定的原则。	
7. 确定最佳的 I&T 决策制定模式。	
8. 确定适当的 I&T 决策授权级别，包括界限规则。	

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI Cybermaturity Platform，2018 年	GE.AG Apply Governance System; GE.MG Monitor Governance System
ISO/IEC 38500:2015(E)	5.2 Principle 1: Responsibility (Evaluate)
ITIL 第 3 版，2011 年	Service Strategy, 2.3 Governance and management systems
美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	3.1 Preparation (Tasks 2, 3, 4, 5)
治理实践	**指标示例**
EDM01.02 指导治理系统。 向领导沟通 I&T 治理原则并获得他们的支持、认同和承诺。根据商定的治理原则、决策模式和权限级别，指导 I&T 治理的结构、流程和实践。定义做出明智决策所需的信息。	a. 流程和实践明确执行商定的 I&T 治理原则的程度（可追溯到原则的流程和实践的百分比） b. 向执行委员会和董事会报告 I&T 治理情况的频率 c. 由适当的业务和 I&T 管理人员定义、分配和接受的 I&T 治理角色、职责和权限的数量

活动	能力级别
1. 沟通 I&T 治理原则，并与高级管理层就如何组建知情且承诺负责的领导层达成共识。	2
2. 根据商定的设计原则建立或委托建立治理结构、流程和实践。	
3. 建立董事会级别的 I&T 治理委员会（或同等组织）。该委员会应确保将信息和技术治理作为企业治理一部分进行适当的处理；提出有关战略方向的建议；并根据企业的业务战略和优先级确定 I&T 促成的投资计划的优先级。	
4. 根据商定的治理设计原则、决策模式和授权，分配 I&T 决策的职责、权限和责任。	3
5. 确保沟通和报告机制为负责监督和决策的人员提供适当的信息。	
6. 指导工作人员遵守相关的道德和职业行为准则，并确保告知和执行不合规行为的后果。	
7. 指导建立激励系统，以推动理想的文化变革。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	GE.DG Direct Governance System
ISF, The Standard of Good Practice for Information Security 2016	SG1.1 Security Governance Framework
ISO/IEC 38500:2015(E)	5.2 Principle 1: Responsibility (Direct)
ISO/IEC 38502:2017(E)	Governance of IT - Framework and model（所有章节）
King IV Report on Corporate Governance for South Africa，2016 年	Part 5.4: Governance functional areas - Principle 12
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.14 Planning (PL-2, PL-10)
治理实践	**指标示例**
EDM01.03 监控治理系统。 监控企业 I&T 治理的有效性和绩效。评估治理系统和实施的机制（包括结构、原则和流程）是否在有效运行，并对 I&T 进行适当的监督，以实现价值创造。	a. 关键决策的实际周期与目标周期 b. 对 I&T 治理进行独立审查的频率 c. 利益相关方的满意度水平（通过调查来衡量） d. 已报告的 I&T 治理问题的数量

A. 组件：流程（续）	
活动	**能力级别**
1. 评估被授予 I&T 治理职责和职权的利益相关方的有效性和绩效。	3
2. 定期评估商定的 I&T 治理机制（结构、原则、流程等）是否已建立并有效运作。	4
3. 评估治理设计的有效性，并制定行动以纠正发现的任何偏差。	
4. 持续监督 I&T 遵守义务（法律、法规、习惯法、合同）、内部政策、标准和专业准则的程度。	
5. 监督企业控制系统的有效性和遵守情况。	
6. 监控常规和例行机制，确保 I&T 的使用符合相关义务（法律、法规、习惯法、合同）、标准和准则。	

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 38500:2015(E)	5.2 Principle 1: Responsibility (Monitor)
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.14 Planning (PL-11)

B. 组件：组织结构					
关键治理实践	董事会	执行委员会	首席执行官	首席信息官	I&T 治理委员会
EDM01.01 评估治理系统。	A	R	R	R	R
EDM01.02 指导治理系统。	A	R			R
EDM01.03 监控治理系统。	A	R	R	R	R

相关指南（标准、框架、合规性要求）	详细参考
COSO Enterprise Risk Management，2017 年 6 月	6. Governance and Culture—Principle 2
ISO/IEC 38502:2017(E)	5.1 Responsibilities of the governing body
King IV Report on Corporate Governance for South Africa，2016 年	Part 2: Fundamental concepts—Definition of corporate governance; Part 5.3: Governing structures and delegation—Principle 6 & 7

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
治理实践	输入		输出	
	自	描述	描述	至
EDM01.01 评估治理系统。	MEA03.02	沟通变更的合规性要求	企业治理指导原则	所有 EDM；APO01.01；APO01.03 APO01.04
	在 COBIT 外部	• 宪法/法律/组织章程 • 治理/决策模式 • 法律/法规 • 业务环境趋势	决策模式	所有 EDM；APO01.01；APO01.04
			权限级别	所有 EDM；APO01.05
EDM01.02 指导治理系统。			企业治理沟通	所有 EDM；APO01.02
			激励系统方法	APO07.03；APO07.04
EDM01.03 监控治理系统。	MEA01.04	绩效报告	关于治理有效性和绩效的反馈	所有 EDM；APO01.11
	MEA01.05	行动的状态和结果		
	MEA02.01	• 内部控制的监控和审查结果 • 基准检测和其他评估的结果		
	MEA02.03	自我评估审查的结果		
	MEA03.03	合规性确认		
	MEA03.04	• 合规性鉴证报告 • 不合规问题和根本原因的报告		
	MEA04.02	鉴证计划		
	在 COBIT 外部	• 审计报告 • 义务		

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-37，修订版 2，2017 年 9 月	3.1 Preparation (Task 2, 3, 4, 5): Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
IS 治理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage—E.9. IS Governance
IT 治理	Skills Framework for the Information Age，第 6 版，2015 年	GOVN

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
授权政策	指定董事会严格保留的权限。列举一般授权原则和授权时间表（包括明确的界限）。定义接受董事会授权的组织结构。	(1) ISO/IEC 38500:2015(E); (2) ISO/IEC 38502:2017(E); (3) King IV Report on Corporate Governance for South Africa，2016 年	(1) 5.2 Principle 1: Responsibility; (2) 5.3 Delegation; (3) Part 5.3: Governing structures and delegation Principle—8 and 10
治理政策	提供治理的指导原则（例如，I&T 治理对企业的成功至关重要；I&T 和业务应保持战略一致性；业务要求和效益决定了优先级；必须公平、及时和一致地执行；必须适当地评估和实施行业最佳实践、框架和标准）。包括为获得成功必须进行的治理，如建立信任和伙伴关系。强调 I&T 治理应反映持续改进流程，必须进行定制、维护和更新，以确保相关性。	美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.14 Planning (PL-1)

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
确定和沟通体现企业价值观的决策文化、组织道德和个人行为。展示道德领导力，表明“高层态度”。	(1) 美国国家标准与技术研究所特别出版物 800-53，修订版 5，2017 年 8 月；(2) ISO/IEC 38500:2015(E)；(3) King IV Report on Corporate Governance for South Africa，2016 年	(1) 3.14 Planning (PL-4); (2) 4.1 Principles; (3) Part 5.1: Leadership, ethics and corporate citizenship - Principle 2

G. 组件：服务、基础设施和应用程序
• COBIT 和相关产品/工具 • 等效框架和标准

领域：评估、指导和监控 治理目标：EDM02 — 确保实现效益	焦点领域：COBIT 核心模型

描述

优化对业务流程、I&T 服务和 I&T 资产的投资为业务创造的价值。

目的

保证从 I&T 促成的举措、服务及资产中获得最佳价值；以经济高效的方式提供解决方案和服务；可靠准确地维护成本和效益信息，从而有效和高效地支持业务需求。

治理目标支持一系列主要企业目标和一致性目标的实现：

企业目标	一致性目标
• EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	AG03 通过 I&T 促成的投资和服务组合所实现的效益

企业目标的指标示例	
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比

一致性目标的指标示例	
AG03	a. 达到或超过业务案例宣称效益的 I&T 促成的投资的百分比 b. 实现预期效益（如服务水平协议所述）的 I&T 服务的百分比

A. 组件：流程

治理实践	指标示例
EDM02.01 建立目标投资组合。 审查并确保企业和 I&T 战略及当前服务的明确性。根据成本、与战略的一致性、组合中计划的效益类型、风险等级以及财务衡量指标（完整经济生命周期中的成本和预期投资回报率 [ROI]）定义适当的投资组合。必要时调整企业和 I&T 战略。	a. 可追溯到企业战略的 I&T 投资的百分比 b. 基于成本、与战略的一致性、财务衡量指标（如完整经济生命周期中的成本和预期 ROI）、风险等级以及组合中计划的效益类型的 I&T 投资的百分比

活动	能力级别
1. 创建并维护 I&T 促成的投资计划、IT 服务和 IT 资产的组合，形成当前 IT 预算的基础，并支持 I&T 战术和战略计划。	2
2. 就推动和支持企业战略的 IT 潜在机会在 IT 和其他业务职能部门之间达成共识。	
3. 确定支持企业战略所需的信息系统、应用程序、数据、IT 服务、基础设施、I&T 资产、资源、技能、实践、控制和关系大类。	
4. 商定 I&T 目标，同时要考虑到企业战略与 I&T 服务、资产及其他资源之间的相互关系。确定并利用可以实现的协同作用。	
5. 定义一个在多个维度之中实现适当平衡的投资组合，包括短期和长期回报、财务和非财务效益、高风险和低风险投资的适当平衡。	3

相关指南（标准、框架、合规性要求）	详细参考
King IV Report on Corporate Governance for South Africa，2016 年	Part 5.5: Stakeholder relationships—Principle 17
The Open Group IT4IT Reference Architecture，第 2.0 版	3.2 IT Value Chain and IT4IT Reference Architecture

A. 组件：流程（续）	
治理实践	**指标示例**
EDM02.02 评估价值优化。 持续评估 I&T 促成的投资、服务和资产的组合，以确定实现企业目标并交付价值的可能性。确定并评估管理方向上的任何变化，以优化价值创造。	a. 目标投资组合与实际投资组合之间的偏差 b. 有可能以合理的成本实现企业目标并交付价值的 I&T 促成的投资组合的百分比

活动	能力级别
1. 了解利益相关者的要求；战略性 I&T 问题，例如对 I&T 的依赖程度；关于 I&T 对企业战略的实际与潜在重要性的技术见解和能力。	2
2. 了解以可靠、安全且具有成本效益的方式从现有和新的 I&T 服务、资产和资源的使用中获得最佳价值所需的关键治理元素。	3
3. 了解并定期讨论当前、新的或新兴技术引起的变化可能给企业带来的机遇，并优化这些机会所创造的价值。	
4. 了解企业价值的构成元素，并思考在整个企业流程中有效沟通、理解和应用此等价值的程度。	
5. 评估企业和 I&T 战略有效地整合到企业内部并与企业的价值实现目标保持一致的程度。	4
6. 了解并考虑当前角色、职责、责任和决策机构在确保 I&T 促成的投资、服务和资产的价值创造方面的效果。	
7. 衡量 I&T 促成的投资、服务和资产的管理与企业价值管理和财务管理实践的一致程度。	
8. 评估投资、服务和资产组合是否符合企业的战略目标；企业的财务和非财务效益；交付风险和效益风险；业务流程的一致性；在可用性、可获取性和响应能力方面的有效性；以及成本、冗余和技术运行状况方面的效率。	

相关指南（标准、框架、合规性要求）	详细参考
COSO Enterprise Risk Management，2017 年 6 月	7. Strategy and Objective-Setting—Principle 8
ISF, The Standard of Good Practice for Information Security 2016	SG2.2 Stakeholder Value Delivery
ISO/IEC 38500:2015(E)	5.3 Principle 2: Strategy (Evaluate)
King IV Report on Corporate Governance for South Africa，2016 年	Part 5.2: Strategy, performance and reporting—Principle 4
The Open Group IT4IT Reference Architecture，第 2.0 版	5. Strategy to Portfolio (S2P) Value Stream

治理实践	指标示例
EDM02.03 指导价值优化。 指导价值管理原则和实践，以便在 I&T 促成投资的完整经济生命周期内能够从投资中实现最佳价值。	a. 对于在整个生命周期内妥当管理其价值的总体组合，I&T 举措在组合中的百分比 b. 使用价值管理原则和实践的 I&T 举措的百分比

活动	能力级别
1. 定义和沟通投资组合和类型、类别、标准以及相对于标准的权重，以获得总体相对价值分数。	2
2. 确定阶段-关卡和其他审查的要求，以确定投资对企业的重要性和相关风险、计划时间表、资金计划，以及关键能力和效益的交付及持续的价值贡献。	3
3. 指导管理层考虑以可能的创新方式使用 I&T，促使企业能够应对新的机遇或挑战、开展新业务、提高竞争力或改进流程。	
4. 指导在分配执行投资组合以及实现业务流程和服务的价值这两方面的职责和责任时所需的任何变更。	
5. 指导任何必要的投资和服务组合变更，以便恢复与当前和预期的企业目标和/或约束条件的一致性。	
6. 建议考虑能够推动企业从 I&T 促成的举措中获取更多价值的潜在创新、组织变更或运营改进。	
7. 定义和传达企业级的价值实现目标和成果衡量指标，以实现有效的监控。	4

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
ISO/IEC 38500:2015(E)	5.3 Principle 2: Strategy (Direct)
治理实践	**指标示例**
EDM02.04 监控价值优化。 监控关键目标和指标，以确定 I&T 促成的投资和服务是否为企业创造了预期价值和效益。识别重大问题并考虑纠正措施。	a. 因 I&T 发展而直接实现的企业的新机会数量 b. 因战略性 I&T 举措而实现的企业战略目标的百分比 c. 高级管理层对 I&T 价值实现和成本的满意度水平 d. 利益相关方对既定目标的进展（基于调查的价值实现）的满意度水平 e. 利益相关方对企业从 I&T 促成的举措获取价值的能力的满意度水平 f. 因实际或故意规避既定的价值管理原则和实践而发生的事故的数量 g. 实现预期价值的百分比

活动	能力级别
1. 定义一组均衡的绩效目标、指标、标的和基准。指标应涵盖活动和成果衡量指标，包括成果的超前和滞后指标，以及财务与非财务衡量指标的适度平衡。与 IT 和其他业务职能部门以及其他利益相关方一同审查这些指标并达成共识。	4
2. 收集相关、及时、完整、可靠且准确的数据来报告实现目标价值的进度。获得简洁、全面和高层次的组合、计划及 I&T（技术和运营能力）绩效视图，为决策提供支持。确保正在实现预期成果。	
3. 定期获取相关的组合、计划和 I&T（技术和职能方面）绩效报告。审查企业既定目标的进展情况，以及实现计划目标、获得交付成果、满足绩效目标和缓解风险的程度。	
4. 审查报告时，确保发起和控制适当的管理纠正行动。	5
5. 审查报告时，根据需要采取适当的管理措施，以确保优化价值。	

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 38500:2015(E)	5.3 Principle 2: Strategy (Monitor)

B. 组件：组织结构								
关键治理实践	**董事会**	**执行委员会**	**首席执行官**	**首席财务官**	**首席运营官**	**首席信息官**	**I&T 治理委员会**	**组合经理**
EDM02.01 建立目标投资组合。	A	R	R	R	R	R	R	
EDM02.02 评估价值优化。	A	R	R	R	R	R	R	
EDM02.03 指导价值优化。	A	R	R	R	R	R	R	
EDM02.04 监控价值优化。	A	R	R	R	R	R	R	R

相关指南（标准、框架、合规性要求）	详细参考	
King IV Report on Corporate Governance for South Africa，2016 年	Part 2: Fundamental concepts—Definition of corporate governance	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
治理实践	输入		输出	
	自	描述	描述	至
EDM02.01 建立目标投资组合。	APO02.05	• 战略举措的定义 • 风险评估举措 • 战略路线图	战略和目标反馈	APO02.05
	APO09.01	标准服务的定义	已确定的支持战略所需的资源和能力	内部
	BAI03.11	服务定义	定义的投资组合	内部；EDM02.03
	EDM02.03	投资类型和标准		
EDM02.02 评估价值优化。	APO02.05	战略路线图	战略一致性的评估	APO02.04；APO05.02
	APO05.01	投资回报预期	投资和服务组合的评估	APO05.02；APO05.03；APO06.02
	APO05.02	包含 ROI 里程碑的精选计划		
	APO05.05	效益结果和相关沟通		
	BAI01.06	阶段-关卡审查结果		
EDM02.03 指导价值优化。	APO05.03	投资组合绩效报告	阶段-关卡审查的需求	BAI01.01；BAI11.01
	EDM02.01	定义的投资组合	投资类型和标准	EDM02.01；APO05.02
EDM02.04 监控价值优化。	APO05.03	投资组合绩效报告	改进实现价值的措施	APO05.03；APO06.02；BAI01.01；BAI11.01；EDM05.01
			组合和计划绩效的反馈	APO05.03；APO06.05；BAI01.06
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
效益管理	Skills Framework for the Information Age，第 6 版，2015 年	BENM

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
预算编制和交付执行政策	制定用于确定投资需求和要求、监控执行情况并确保实现最大利益的准则。制定预算请求。根据计划监控预算和技术绩效的执行情况。在有合理依据的情况下提出重新分配或调整计划的建议。根据服务水平协议和其他基于绩效的指标对绩效进行监控。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
I&T 增加的价值取决于 I&T 与业务保持一致并满足其期望的程度。建立在预算内准时交付相应质量的 I&T 服务的文化，以优化 I&T 价值。		

G. 组件：服务、基础设施和应用程序
• 成本会计系统 • 计划管理工具

领域：评估、指导和监控 治理目标：EDM03 — 确保风险优化	焦点领域：COBIT 核心模型

描述

确保理解、明确说明和传达企业的风险偏好与容忍度，并识别和管控使用 I&T 给企业价值带来的风险。

目的

确保 I&T 相关企业风险不超过企业的风险偏好和风险容忍度，识别和管控 I&T 风险对企业价值的影响，以及最大程度地降低不合规的可能性。

治理目标支持一系列主要企业目标和一致性目标的实现：

企业目标	一致性目标
• EG02 妥当管理的业务风险 • EG06 业务服务连续性和可用性	• AG02 妥当管理的 I&T 相关风险 • AG07 信息、参与执行的基础设施和应用程序的安全，以及隐私的安全

企业目标的指标示例		一致性目标的指标示例	
EG02	a. 风险评估涵盖的关键业务目标和服务的百分比 b. 风险评估未发现的重大事故数量与总事故数量的比率 c. 风险概况的更新频率	AG02	a. 风险概况的更新频率 b. 涵盖 I&T 相关风险的企业风险评估的百分比 c. 风险评估中未识别的 I&T 相关重大事故的数量
EG06	a. 导致重大事故的客户服务或业务流程中断的次数 b. 事故的业务成本 c. 因计划外服务中断而损失的业务处理小时数 d. 与承诺的服务可用性目标有关的投诉百分比	AG07	a. 导致财务损失、业务中断或公众形象受损的保密性事故的数量 b. 导致财务损失、业务中断或公众形象受损的可用性事故的数量 c. 导致财务损失、业务中断或公众形象受损的完整性事故的数量

A. 组件：流程

治理实践	指标示例
EDM03.01 评估风险管理。 持续检查和评估当前和未来在企业中使用 I&T 的风险效应。考虑企业的风险偏好是否适合，并确保与 I&T 使用相关的企业价值风险得到识别和管理。	a. 意外企业影响的水平 b. 超出企业风险容忍度的 I&T 风险的百分比 c. 风险因素评估的更新率

活动	能力级别
1. 了解组织及其 I&T 风险相关的背景。	2
2. 确定企业的风险偏好，即企业为实现其目标而愿意承担的 I&T 相关风险的水平。	
3. 确定相对风险偏好的风险容忍度，即暂时可接受的与风险偏好的偏离水平。	
4. 确定 I&T 风险战略与企业风险战略的一致程度，并确保风险偏好低于组织的风险能力。	
5. 在企业战略决策未决之前主动评估 I&T 风险因素，并确保企业的战略决策流程将风险纳入考虑。	3
6. 评估风险管理活动，确保与企业的 I&T 相关损失承受力及领导层对此损失的容忍度保持一致。	
7. 吸引并维护 I&T 风险管理所需的技能和人员	

相关指南（标准、框架、合规性要求）	详细参考
COSO Enterprise Risk Management，2017 年 6 月	Strategy and Objective-Setting—Principles 6 and 7; 9. Review and Revision—Principle 16

A. 组件：流程（续）	
治理实践	**指标示例**
EDM03.02 指导风险管理。 指导风险管理实践的建立，提供合理的保障，确保 I&T 风险管理实践是适当的且实际的 I&T 风险不超过董事会的风险偏好。	a. I&T 风险与企业风险之间的一致性水平 b. 涵盖 I&T 风险的企业项目的百分比

活动	能力级别
1. 指导将 I&T 风险战略转化和整合到风险管理实践和运营活动中。	2
2. 指导风险沟通计划（覆盖企业的各个层面）的制定。	
3. 指导适当机制的实施，以迅速应对不断变化的风险，并根据商定的上报原则（报告内容、时间、地点和方式）立即向相应的管理层报告。	
4. 指示任何人可随时向相关方报告其发现的风险、机会、问题和顾虑。应根据公布的政策和程序管理风险，并上报给相关决策者。	
5. 确定要监控的风险治理和管理流程的关键目标和指标，并批准用于获取和报告衡量信息的方式、方法、技术和流程。	3

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	RS.AS Apply Risk Management Strategy; BC.RO Determine Strategic Risk Objectives
ISF, The Standard of Good Practice for Information Security 2016	IR1.1 Information Risk Assessment—Management Approach
King IV Report on Corporate Governance for South Africa，2016 年	Part 5.4: Governance functional areas—Principle 11
美国国家标准与技术研究所特别出版物 800-37， 修订版 2（草稿），2018 年 5 月	3.5 Assessment (Task 2)

治理实践	指标示例
EDM03.03 监控风险管理。 监控风险管理流程的关键目标和指标。确定如何识别、追踪或报告偏差或问题以进行补救。	a. 已识别和管理的潜在 I&T 风险领域的数量 b. 已有效缓解的关键风险的百分比 c. 及时执行的 I&T 风险行动计划的百分比

活动	能力级别
1. 向董事会或执行委员会报告任何风险管理问题。	2
2. 监控在企业的风险偏好阈值和容忍度阈值范围内的风险概况管理水平。	3
3. 针对目标监控风险治理和管理流程的关键目标和指标，分析任何偏离的原因并采取补救措施解决问题的根源。	4
4. 使关键利益相关方能够审查企业既定目标的进展情况。	

相关指南（标准、框架、合规性要求）	详细参考
COSO Enterprise Risk Management，2017 年 6 月	9. Review and Revision—Principle 17
美国国家标准与技术研究所特别出版物 800-37， 修订版 2（草稿），2018 年 5 月	3.1 Preparation (Task 7); 3.5 Assessment (Task 1); 3.6 Authorization (Task 1)
The Open Group IT4IT Reference Architecture，第 2.0 版	6. Requirement to Deploy (R2D) Value Stream; 7. Request to Fulfill (R2F) Value Stream

B. 组件：组织结构								
关键治理实践	董事会	执行委员会	首席执行官	首席风险官	首席信息官	I&T 治理委员会	企业风险委员会	首席信息安全官
EDM03.01 评估风险管理。	A	R	R	R	R	R	R	
EDM03.02 指导风险管理。	A	R	R	R	R	R	R	
EDM03.03 监控风险管理。	A	R	R	R	R	R	R	R

相关指南（标准、框架、合规性要求）	详细参考
COSO Enterprise Risk Management，2017 年 6 月	6. Governance and Culture—Principle
King IV Report on Corporate Governance for South Africa，2016 年	Part 2: Fundamental concepts—Definition of corporate governance

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
治理实践	输入		输出	
	自	描述	描述	至
EDM03.01 评估风险管理。	APO12.01	新出现的风险问题和因素	风险偏好的指导准则	APO04.01；APO12.03
	在 COBIT 外部	企业风险管理 (ERM) 原则	风险管理活动的评估	APO12.01
			已批准的风险容忍度水平	APO12.03
EDM03.02 指导风险管理。	APO12.03	汇总的风险概况，包括风险管理行动的状态	已批准的风险管理衡量流程	APO12.01
	在 COBIT 外部	企业风险管理 (ERM) 概况和缓解计划	需要监控的风险管理关键目标	APO12.01
			风险管理政策	APO12.01
EDM03.03 监控风险管理。	APO12.02	风险分析结果	解决风险管理偏离的补救措施	APO12.06
	APO12.04	• 面向利益相关方的风险分析和风险概况报告 • 第三方风险评估的结果 • 接受更高风险的机会	报告给董事会的风险管理问题	EDM05.01

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-37，修订版 2，2017 年 9 月	3.1 Preparation (Task 7): Inputs and Outputs; 3.5 Assessment (Tasks 1, 2): Inputs 2, and Outputs; 3.6 Authorization (Task 1): Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
业务风险管理	Skills Framework for the Information Age，第 6 版，2015 年	BURM
风险管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage—E.3. Risk Management

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
企业风险政策	在战略、策略和运营层面定义与业务目标一致的企业风险治理和管理。将企业治理转化为风险治理原则和政策，并详细阐述风险管理活动。	美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.17 Risk assessment (RA-1)

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
培养组织各个层面的 I&T 风险意识文化，使企业能够主动识别、报告和上报 I&T 风险、机会和潜在的业务影响。高级管理层设定方向并为风险实践提供明确和切实的支持。此外，管理层必须明确界定风险偏好，并营造合理程度的讨论氛围，作为正常业务活动的一部分。理想行为包括鼓励员工提出问题或负面结果，并展示 I&T 风险的透明度。业务所有者应在适用时接受 I&T 风险的所有权，并通过提供充足的资源来展示对 I&T 风险管理的切实承诺。	COSO Enterprise Risk Management，2017 年 6 月	6. Governance and Culture—Principles 3 and 4

G. 组件：服务、基础设施和应用程序
风险管理系统

领域：评估、指导和监控 治理目标：EDM04 — 确保资源优化	焦点领域：COBIT 核心模型

描述

确保以最佳的成本效益提供适当且充足的业务和 I&T 相关资源（人员、流程和技术）来支持企业目标。

目的

确保以最优的方式满足企业的资源需求，优化 I&T 成本，提高效益实现的可能性，并为未来的改变做好准备。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	AG09 在预算内按时交付计划且满足要求和质量标准

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG09	a. 在预算内按时交付的计划/项目的数量 b. 因质量缺陷需要重大返工的计划的数量 c. 对计划/项目质量满意的利益相关方的百分比
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比		

A. 组件：流程

治理实践	指标示例
EDM04.01 评估资源管理。 持续检查和评估当前与未来对业务和 I&T 资源（财务和人力）的需求、资源选项（包括资源采购战略）以及分配和管理原则，从而以最佳的方式满足企业需求。	a. 与资源计划的偏差数量 b. 使用分配的资源交付价值并缓解风险的资源计划和企业架构战略的百分比

活动	能力级别
1. 从当前和未来战略开始，检查提供 I&T 相关资源（技术、财务和人力资源）的潜在方案，并拓展满足当前和未来需求的能力（包括采购方案）。	2
2. 定义资源分配以及资源和能力管理的关键原则，使 I&T 能够根据商定的优先级和预算限制来满足企业的需求。例如，定义特定服务的首选采购方案以及每个采购方案的财务限制。	
3. 审查和批准使用分配的资源交付价值并缓解风险的资源计划和企业架构战略。	
4. 了解 I&T 资源管理与企业财务和人力资源 (HR) 计划保持一致的要求。	
5. 定义企业架构的管理和控制原则。	3

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	GR.DR Direct Resource Management Needs
ISO/IEC 38500:2015(E)	5.4 Principle 3: Acquisition (Evaluate)

A. 组件：流程（续）	
治理实践	**指标示例**
EDM04.02 指导资源管理。 确保采用资源管理原则，促使业务和 I&T 资源在完整经济生命周期得到最佳利用。	a. 与资源管理原则的偏差和例外情况的数量 b. 架构组件复用的百分比

活动	能力级别
1. 分配执行资源管理的职责。	2
2. 制定与资源保护有关的原则。	
3. 沟通并推动资源管理战略、原则以及商定的资源计划和企业架构战略的采用。	3
4. 使资源管理与企业财务和人力资源计划保持一致。	
5. 定义资源管理的关键目标、衡量方式和指标。	4

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	GR.ER Evaluate Resource Management Needs
COSO Enterprise Risk Management，2017 年 6 月	6. Governance and Culture—Principle 5
ISO/IEC 38500:2015(E)	5.4 Principle 3: Acquisition (Direct)
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.14 Planning (PL-4)

治理实践	指标示例
EDM04.03 监控资源管理。 监控资源管理流程的关键目标和指标。确定如何识别、追踪或报告偏差或问题以进行补救。	a. 利益相关方对资源优化的反馈水平 b. 通过优化资源使用实现的效益（例如成本节省）的数量 c. 已实现的资源管理绩效目标的数量 d. 由于资源管理问题而导致中等或高风险状态的项目和计划的百分比 e. 已分配适当资源的项目的百分比

活动	能力级别
1. 根据企业目标和优先级使用商定的目标和指标来监控资源的分配和优化。	4
2. 监控 I&T 相关的采购策略、企业架构战略以及业务和 IT 相关能力和资源，以确保满足当前和未来的企业需求和目标。	
3. 根据目标监控资源绩效，分析偏差原因，并通过补救措施解决问题的根源。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	GR.MR Monitor Resource Management Needs
ISO/IEC 38500:2015(E)	5.4 Principle 3: Acquisition (Evaluate)

B. 组件：组织结构							
关键治理实践	董事会	执行委员会	首席执行官	首席运营官	首席信息官	I&T 治理委员会
EDM04.01 评估资源管理。	A	R	R	R	R	R
EDM04.02 指导资源管理。	A	R	R	R	R	R
EDM04.03 监控资源管理。	A	R	R	R	R	R

相关指南（标准、框架、合规性要求）	详细参考
King IV Report on Corporate Governance for South Africa，2016 年	Part 2: Fundamental concepts—Definition of corporate governance

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
治理实践	输入		输出	
EDM04.01 评估资源管理。	自	描述	描述	至
	APO02.04	为实现目标能力需弥补的差距和做出的改变	资源和能力分配的指导原则	APO02.01；APO07.01；BAI03.11
	APO07.03	技能培养计划	已批准的资源计划	APO02.05；APO07.01；APO09.02
	APO10.02	供应商评估的决策结果	企业架构的指导原则	APO03.01
EDM04.02 指导资源管理。			资源保护原则	APO01.02
			分配的资源管理职责	APO01.05；DSS06.03
			资源配置战略的沟通	APO02.06；APO07.05；APO09.02
EDM04.03 监控资源管理。			解决资源管理偏离的补救措施	APO02.05；APO07.01；APO07.03；APO09.04
			对资源和能力分配及有效性的反馈	EDM05.01；APO02.02；APO07.05；APO09.05

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
组合管理	Skills Framework for the Information Age，第 6 版，2015 年	POMG
资源配置	Skills Framework for the Information Age，第 6 版，2015 年	RESC

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
绩效衡量政策	识别对超越传统会计的绩效衡量系统的需求。这种系统涵盖对在信息时代参与竞争所需的关系和知识资产的衡量，包括以客户为中心、流程效率以及学习和成长的能力（平衡计分卡）。平衡计分卡考虑客户满意度、简化企业的内部职能、提高运营效率和拓展工作人员技能等无形因素，将战略转化为行动以实现企业目标。这种全面的运营视角有助于将长期战略目标与短期行动联系起来。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
建立重视资源并且资源（人员、信息、应用程序、技术或设施）的投资、使用和分配与组织需求保持一致的文化。通过确保组织中存在适当的方法和充分的技能来展现这些价值；例如，确保服务采购的效益真实存在且可以实现，以及实施合理的绩效衡量系统（例如平衡计分卡）。		

G. 组件：服务、基础设施和应用程序
绩效衡量系统（例如平衡计分卡、技能管理工具）

领域：评估、指导和监控 治理目标：EDM05 — 确保利益相关方参与	焦点领域：COBIT 核心模型

描述

确保识别利益相关方并使其参与到 I&T 治理系统中；确保企业 I&T 绩效和一致性衡量与报告是透明的，并且利益相关方批准目标和指标以及必要的补救措施。

目的

确保利益相关方支持 I&T 战略和路线图；与利益相关方保持及时有效的沟通；以及建立报告基础以提高绩效。识别待改进的领域，并确认 I&T 相关目标和战略与企业战略保持一致。

治理目标支持一系列主要企业目标和一致性目标的实现：

企业目标		一致性目标	
• EG04 财务信息的质量 • EG07 管理信息的质量		AG10	I&T 管理信息的质量
企业目标的指标示例		**一致性目标的指标示例**	
EG04	a. 有关企业财务信息的透明度、了解度和准确性的关键利益相关方满意度调查 b. 不遵守财务相关法规的成本	AG10	a. 考虑到可用资源，用户对 I&T 相关管理信息的质量、及时性和可用性的满意度水平 b. 主要因 I&T 相关信息错误或不可用导致的错误业务决策的比率和程度 c. 满足质量准则的信息的百分比
EG07	a. 董事会和执行管理层对决策信息的满意度 b. 基于不准确信息的错误业务决策所导致的事故数量 c. 为有效业务决策提供支持性信息所花的时间 d. 管理信息的及时性		

A. 组件：流程

治理实践	指标示例
EDM05.01 评估利益相关方的参与和报告要求。 持续检查和评估当前及未来关于利益相关方参与和报告（包括监管机构强制要求的报告）的要求以及与其他利益相关方的沟通。制定利益相关方的参与和沟通原则。	a. 上次修订报告要求的日期 b. 报告要求中涵盖的利益相关方百分比

活动	能力级别
1. 识别企业内外所有相关的 I&T 利益相关方。以要求类似为指导，对利益相关方进行分组。	2
2. 检查并评判当前和未来有关企业内 I&T 使用的强制性报告要求（法律、法规、习惯法、合同），包括范围和频率。	
3. 检查并评判其他利益相关方当前和未来有关企业内 I&T 使用的沟通和报告要求，包括要求的参与/咨询水平以及沟通范围/详细程度和条件。	
4. 维护与外部和内部利益相关方的沟通原则（包括沟通格式和渠道），以及利益相关方接受和签字确认报告的原则。	3

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	SR.DR Direct Stakeholder Communication and Reporting

A. 组件：流程（续）	
治理实践	**指标示例**
EDM05.02 指导利益相关方的参与、沟通和报告。 确保建立有效的利益相关方参与、沟通和报告，包括确保信息质量和完整性的机制、强制性报告监督以及为利益相关方制定沟通战略。	a. 违反强制性报告要求的次数 b. 利益相关方对沟通和报告的满意度

活动	能力级别
1. 指导建立面向外部和内部利益相关方的咨询与沟通战略。	2
2. 指导实施确保信息符合企业强制性 I&T 报告要求的所有标准的机制。	
3. 建立强制性报告验证和批准机制。	
4. 建立报告上报机制。	3

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	SR.AR Apply Stakeholder Reporting Requirements
King IV Report on Corporate Governance for South Africa，2016 年	Part 5.5: Stakeholder relationships—Principle 16
King IV Report on Corporate Governance for South Africa，2016 年	Part 5.2: Strategy, performance and reporting—Principle 5
美国国家标准与技术研究所，Framework for Improving Critical Infrastructure Cybersecurity，第 1.1 版，2018 年 4 月	3.3 Communicating Cybersecurity Requirements with Stakeholders

治理实践	指标示例
EDM05.03 监控利益相关方的参与。 监控利益相关方的参与水平和沟通的有效性。评估用于确保准确性、可靠性和有效性的机制以及确定不同利益相关方的报告和沟通要求是否得到满足。	a. 利益相关方在企业 I&T 方面的参与水平 b. 包含不准确内容的报告的百分比 c. 按时交付的报告的百分比

活动	能力级别
1. 定期评估机制的有效性以确保强制性报告的准确性和可靠性。	4
2. 定期评估内外部利益相关方参与和沟通机制的有效性以及成果。	
3. 确定不同利益相关方的要求是否得到满足并评估利益相关方的参与水平。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	SR.MC Monitor Stakeholder Communication

B. 组件：组织结构					
关键治理实践	董事会	执行委员会	首席执行官	首席风险官	首席信息官
EDM05.01 评估利益相关方的参与和报告要求。	A	R	R	R	R
EDM05.02 指导利益相关方的参与、沟通和报告。	A	R	R	R	R
EDM05.03 监控利益相关方的参与。	A	R	R	R	R

相关指南（标准、框架、合规性要求）	详细参考
King IV Report on Corporate Governance for South Africa，2016 年	Part 2: Fundamental concepts—Definition of corporate governance

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
治理实践	输入		输出	
EDM05.01 评估利益相关方的参与和报告要求。	自	描述	描述	至
	EDM02.04	改进实现价值的措施	报告和沟通原则	MEA01.01
	EDM03.03	报告给董事会的风险管理问题	企业报告要求评估	MEA01.01
	EDM04.03	对资源和能力分配及有效性的反馈		
EDM05.02 监控利益相关方的参与、沟通和报告。	APO12.04	面向利益相关方的风险分析和风险概况报告	验证和批准强制性报告的规则	MEA01.01；MEA03.04
			上报指南	MEA01.05
EDM05.03 监控利益相关方的参与。	MEA04.08	• 鉴证审查结果 • 鉴证审查报告	报告有效性的评估	MEA01.01；MEA03.04
相关指南（标准、框架、合规性要求）		详细参考		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
关系管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage—E.4. Relationship Management

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
透明度政策	阐述了与所有利益相关方进行频繁和开放的沟通的重要性，以确保他们了解 I&T 对企业成功的战略重要性。确保利用该透明度支持适当的风险缓解，将透明度和有效的风险管理与 I&T 价值和企业发展联系起来。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
营造根据利益相关方的要求与其进行开放且条理清晰的沟通文化。		

G. 组件：服务、基础设施和应用程序
• 沟通工具和渠道 • IT 仪表盘 • 利益相关方调查工具

4.2 调整、规划和组织 (APO)

01 妥当管理的 I&T 管理框架
02 妥当管理的战略
03 妥当管理的企业架构
04 妥当管理的创新
05 妥当管理的组合
06 妥当管理的预算和成本
07 妥当管理的人力资源
08 妥当管理的关系
09 妥当管理的服务协议
10 妥当管理的供应商
11 妥当管理的质量
12 妥当管理的风险
13 妥当管理的安全
14 妥当管理的数据

领域：调整、规划和组织 管理目标：APO01 — 妥当管理的 I&T 管理框架	焦点领域：COBIT 核心模型

描述

根据企业目标和其他设计因素设计企业的 I&T 管理系统。基于此设计，实施管理系统的所有必需组件。

目的

实施一致的管理方法，以满足企业治理需求，涵盖治理组件，如管理流程；组织结构；角色和职责；可靠且可重复的活动；信息项目；政策和程序；技能和能力；文化和行为；以及服务、基础设施和应用程序。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG03 遵守外部法律和法规 • EG08 内部业务流程功能的优化 • EG11 遵守内部政策 • EG12 妥当管理的数字化转型计划	• AG03 通过 I&T 促成的投资和服务组合所实现的效益 • AG11 I&T 遵守内部政策

企业目标的指标示例		一致性目标的指标示例	
EG03	a. 不合规的成本，包括结算和罚款 b. 引起负面舆论或负面影响的不合规问题的数量 c. 监管机构指出的违规问题的数量 d. 与业务伙伴合同协议有关的不合规问题的数量	AG03	a. 达到或超过业务案例宣称效益的 I&T 促成的投资的百分比 b. 实现预期效益（如服务水平协议所述）的 I&T 服务的百分比
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度	AG11	a. 与违反 I&T 相关政策有关的事故的数量。 b. 内部政策的例外情况的数量 c. 政策审查和更新的频率
EG11	a. 与违反政策有关的事故的数量 b. 了解政策的利益相关方的百分比 c. 得到有效标准和工作实践支持的政策的百分比		
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比		

A. 组件：流程	
管理实践	**指标示例**
APO01.01 设计企业 I&T 的管理系统。 设计适合企业需求的管理系统。使用目标级联并应用设计因素来定义企业的管理需求。确保治理组件与企业的治理和管理理念以及运营风格融合并保持一致。	a. 由适用治理结构正式签字确认的 I&T 管理系统优先目标的数量 b. 治理组件与企业的治理和管理理念以及运营风格融合并保持一致的百分比

活动	能力级别
1. 了解企业愿景、方向和战略以及当前的企业背景和挑战。	2
2. 考虑到企业的内部环境，包括管理文化和理念、风险容忍度、安全和隐私政策、道德价值观、行为准则、问责制以及管理完整性要求。	
3. 将 COBIT 目标级联和设计因素应用于企业战略和背景，以确定管理系统的优先级，进而确定优先管理目标的实施优先级。	
4. 利用行业特定的良好实践或要求（例如，行业特定法规）和适当的治理结构来验证选定的管理目标的实施优先级。	3

相关指南（标准、框架、合规性要求）	详细参考
COSO Enterprise Risk Management，2017 年 6 月	7. Strategy and Objective-Setting—Principle 9
ISO/IEC 27001:2013/Cor.2:2015(E)	International standard for establishing, implementing and maintaining a management system（所有章节）
ITIL 第 3 版，2011 年	Service Strategy, 2.3 Governance and management systems

管理实践	指标示例
APO01.02 沟通管理目标、方向和决策。 与整个企业的利益相关方沟通，让他们了解和理解一致性目标和 I&T 目标。定期沟通重要的 I&T 相关决策及其对组织的影响。	a. 关于 I&T 管理目标和方向的沟通频率 b. 分配的定期沟通职责

活动	能力级别
1. 提供充足的技能性资源来支持沟通流程。	2
2. 识别沟通需求并基于这些需求实施计划，以定义沟通的基本规则，涵盖自上而下、自下而上和横向的沟通。	3
3. 持续沟通 I&T 目标和方向。通过所有可用的渠道，确保执行管理层在言行上支持沟通。	
4. 确保传达的信息包含明确的使命、服务目标、内部控制、质量、行为/道德规范、政策和程序、角色和责任等。以适当的详细程度向企业内不同的受众群体传达信息。	

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
APO01.03 实施管理流程（以支持治理和管理目标的实现）。 根据管理系统的设计，定义流程能力级别目标和实施优先级。	a. 为实现能力级别目标应实施或改进的优先流程的数量 b. 为成功流程实施的后续行动定义的指标的数量

活动	能力级别
1. 根据优先级管理目标的选择（目标级联和设计因素练习的输出），开发特定于组织的 I&T 治理目标流程模型。	2
2. 分析组织的目标流程模型与当前的实践和活动之间的差距。	3
3. 为缺失的流程实践和活动制定实施路线图。使用实践指标来跟进成功的实施。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO01.04 定义并实施组织结构。 根据管理系统的设计建立所需的内部和扩展组织结构（例如，委员会），从而实现有效和高效的决策。确保管理结构的组成包含所需的技术和信息知识。	a. 执行管理层对管理决策的满意度 b. 管理结构无法解决的已上报至治理结构的决策的数量

活动	能力级别
1. 确定实现企业成果和 I&T 战略以及 I&T 服务管理和执行所需的决策。	2
2. 让对决策至关重要的利益相关方（执行人、责任人、咨询人以及被通知人）参与进来。	
3. 根据治理方向定义 I&T 相关组织内各项职能的范围、重点、要求和职责。	
4. 定义涵盖所有实践（包括第三方执行的实践）所需的内部和外部职能、内部和外部角色以及能力和决策权的范围。	3
5. 使 I&T 相关组织与企业架构组织模型保持一致。	
6. 建立由执行、业务和 I&T 管理层组成的 I&T 指导委员会（或同等组织），以跟踪项目状态、解决资源冲突，以及监控服务水平和服务改进。	
7. 为每个管理结构提供准则（包括要求、目标、与会人员、时间安排、跟踪、监督和督导）以及必要的会议输入和预期的会议成果。	
8. 定期验证组织结构的充分性和有效性。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
APO01.05 确立角色和职责。 定义并沟通企业 I&T 角色和职责，包括权限级别、职责和责任。	a. 分配到个人的 I&T 相关角色的数量 b. 已完成的角色描述的数量

活动	能力级别
1. 根据业务需求和目标，确立、商定和沟通企业所有人员的 I&T 相关角色和职责。清晰描述他们的责任和职责，尤其是决策和审批方面的责任和职责。	2
2. 定义角色时考虑到企业和 I&T 服务连续性要求，包括人员备份和交叉培训要求。	
3. 维护企业内最新的联系信息和角色描述，从而为 I&T 服务连续性流程提供输入。	
4. 在角色和职责描述中添加必须遵守管理政策和程序、道德规范以及专业实践的具体要求。	
5. 确保通过角色和职责定义责任。	
6. 设计角色和职责，降低单个角色危害关键流程的可能性。	
7. 实施适当的监督措施，以确保角色和职责得到适当的履行；评估是否所有人都有足够的权限和资源来履行其角色和职责；并对绩效进行全面审查。监督水平应与所分配职责的职位敏感性和职责范围保持一致。	3

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO01.06 优化 IT 职能的设置。 确定 IT 能力在整个组织结构中的位置，以反映 IT 在企业内的战略重要性和运营依赖性。CIO 和高级管理层 IT 代表的报告层级关系应与 I&T 在企业内的重要性相称。	a. 签字同意设置 IT 职能的利益相关方的数量 b. 对设置 IT 职能持赞成意见的利益相关方的数量

活动	能力级别
1. 了解 IT 职能设置的背景，包括评估企业战略和运营模式（集中、联合、分散、混合）、I&T 的重要性，以及采购情况和方案。	3
2. 确定和评估组织设置、采购和运营模式的方案并确定优先级。	
3. 定义 IT 职能的设置并达成共识。	

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 27002:2013/Cor.2:2015(E)	8.2 Information classification

管理实践	指标示例
APO01.07 定义信息（数据）和系统所有权。 定义和维护信息（数据）及信息系统的所有权。确保所有者对信息和系统进行分类，并按照分类提供保护。	a. 已明确定义所有者的数据资产的百分比 b. 已明确定义所有者的信息系统的百分比 c. 已根据商定的分类级别进行分类的信息项的百分比

活动	能力级别
1. 提供指导原则，确保对整个企业的信息项进行适当和一致的分类。	3
2. 创建和维护包含所有者、保管人和分类列表的信息（系统和数据）清单。包括已外包的系统和企业应保留所有权的系统。	
3. 评估并区分关键（高价值）和非关键的数据、信息和系统。确保为每个类别提供适当的保护。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
APO01.08 定义技能和能力目标。 定义实现相关管理目标所需的技能和能力。	a. 参加过关于特定技能、能力和理想行为的培训或意识课程的员工的数量 b. 具备实现选定管理目标所需的技能和能力的员工的数量

活动	能力级别
1. 确定实现选定管理目标所需的技能和能力。	2
2. 分析企业员工现有技能与目标技能和能力之间的差距。关于技能培养和管理实践，请参阅“APO07 — 妥当管理的人力资源”。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO01.09 定义并沟通政策和程序。 落实程序，维护政策与控制框架中其他组件的合规性以及政策的绩效衡量。强制执行不合规或绩效不足的后果。跟踪趋势与绩效并在控制框架的未来设计和改进中予以考虑。	a. 有记录且保持更新的有效政策和程序的百分比 b. 了解并展现出在政策和程序方面的能力的员工的数量

活动	能力级别
1. 制定一套政策来推动对相关关键主题的 IT 控制期望，例如质量、安全、隐私、内部控制、I&T 资产的使用、道德和知识产权 (IP) 等主题。	3
2. 推出并统一实施面向所有相关员工的 I&T 政策，使其融入并成为企业运营不可或缺的一部分。	
3. 评估和更新政策（至少每年一次），以适应不断变化的运营或商业环境。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO01.10 定义并实施服务、基础设施和应用程序，以支持治理和管理系统。 定义并实施基础设施、服务和应用程序（例如架构贮存库、风险管理系统、项目管理工具、成本跟踪工具和事故监视工具）来支持治理和管理系统。	a. 选定用于支持优先流程的工具的数量 b. 关键 I&T 流程的工具的充分性/覆盖范围 c. 接收者对信息的准确性、完整性和及时性的满意度 d. 利益相关方对选定用于支持其需求的工具感到满意的百分比

活动	能力级别
1. 确定可通过服务、应用程序或基础设施自动化实现的优先管理目标。	2
2. 选择和实施最合适的工具并与利益相关方沟通。	
3. 必要时提供关于所选工具的培训。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
APO01.11 管理 I&T 管理系统的持续改进。 持续改进流程和其他管理系统组件，确保它们能够实现治理和管理目标。考虑 COBIT 实施指南、新兴标准、合规性要求、自动化机会以及利益相关方的反馈。	a. 框架和组件的最新更新日期 b. 由于控制环境设计不当造成的 I&T 相关损失的数量

活动	能力级别
1. 定期评估框架组件的绩效并采取适当措施。	4
2. 根据绩效和一致性驱动因素以及相关风险确定关键业务流程。评估能力并确定改进目标。分析能力和控制方面的差距。确定改进或重新设计流程的方案。	
3. 根据潜在效益和成本确定改进举措的优先级。按常规业务实践实施商定的改进措施，并设定绩效目标和指标来监控改进情况。	5
4. 考虑提高效率和有效性的方法（例如培训、文档、标准化和/或流程自动化）。	
5. 应用质量管理实践来更新流程。	
6. 停用过时的治理组件（流程、信息项、政策等）。	

相关指南（标准、框架、合规性要求）	详细参考
ITIL 第 3 版，2011 年	Continual Service Improvement, 4.1 The 7-Step Improvement Process

B. 组件：组织结构																						
关键管理实践	执行委员会	首席风险官	首席信息官	首席技术官	首席数字官	I&T 治理委员会	架构委员会	企业风险委员会	首席信息安全官	业务流程所有者	数据管理职能部门	人力资源总监	关系经理	架构总监	开发总监	IT 运营总监	IT 行政总监	服务经理	信息安全经理	业务连续性经理	隐私官
APO01.01 设计企业 I&T 的管理系统。	A		R	R	R	R															
APO01.02 沟通管理目标、方向和决策。	A	R	R	R	R	R			R				R								
APO01.03 实施管理流程（以支持治理和管理目标的实现）。	A	R	R	R	R	R			R												
APO01.04 定义并实施组织结构。	A		R	R	R	R						R									
APO01.05 确立角色和职责。	A		R	R	R	R															
APO01.06 优化 IT 职能的设置。	A		R	R	R	R		R													
APO01.07 定义信息（数据）和系统所有权。	A		R	R	R	R		R		R	R			R							
APO01.08 定义技能和能力目标。	A		R	R	R	R								R	R	R	R				
APO01.09 定义并沟通政策和程序。	A		R	R	R	R	R	R		R	R	R		R	R	R	R	R	R	R	R
APO01.10 定义并实施服务、基础设施和应用程序，以支持治理和管理系统。	A		R	R	R	R					R			R	R	R	R	R	R	R	R
APO01.11 管理 I&T 管理系统的持续改进。	A		R	R	R	R				R	R			R	R	R	R	R	R	R	R

B. 组件：组织结构（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
COSO Enterprise Risk Management，2017 年 6 月	6. Governance and Culture—Principle 2
ISO/IEC 27001:2013/Cor.2:2015(E)	5.3 Organizational roles, responsibilities and authorities

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	**输入**		**输出**	
	自	**描述**	**描述**	**至**
APO01.01 设计企业 I&T 的管理系统。	APO02.05	战略路线图	优先的治理和管理目标	所有 APO；所有 BAI；所有 DSS；所有 MEA
	APO12.01	新出现的风险问题和因素	管理系统的设计	所有 APO；所有 BAI；所有 DSS；所有 MEA
	APO12.02	风险分析结果		
	EDM01.01	• 企业治理指导原则 • 决策模式		
APO01.02 沟通管理目标、方向和决策。	APO12.06	风险影响的沟通	沟通的基本规则	所有 APO；所有 BAI；所有 DSS；所有 MEA
	DSS04.01	业务连续性政策和目标	关于 I&T 目标的沟通	所有 APO；所有 BAI；所有 DSS；所有 MEA
	DSS05.01	恶意软件预防政策		
	DSS05.02	连接安全政策		
	DSS05.03	终端设备的安全政策		
	EDM01.02	企业治理沟通		
	EDM04.02	资源保护原则		
APO01.03 实施管理流程（以支持治理和管理目标的实现）。	APO02.04	为实现目标能力需弥补的差距和做出的改变	目标模型差距分析	所有 APO；所有 BAI；所有 DSS；所有 MEA
	EDM01.01	企业治理指导原则	流程能力级别	APO01.11
APO01.04 定义并实施组织结构。	APO03.02	流程架构模型	企业运营准则	APO03.02
	EDM01.01	企业治理指导原则	组织结构和职能的定义	APO03.02

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
	自	**描述**	**描述**	**至**
APO01.05 确立角色和职责。	APO07.03	• 技能和能力矩阵 • 技能培养计划	监督实践的定义	APO07.01
	APO11.01	质量管理系统 (QMS) 的角色、职责和决策权	I&T 相关角色和职责的定义	DSS05.04
	APO13.01	信息安全管理系统 (ISMS) 的范围声明		
	DSS06.03	• 已分配的角色和职责 • 已分配的权限级别		
	EDM01.01	权限级别		
	EDM04.02	分配的资源管理职责		
APO01.06 优化 IT 职能的设置。	在 COBIT 外部	• 企业战略 • 企业运营模式	已定义的 IT 职能的运营设置	APO03.02
			IT 组织方案的评估	APO03.02
APO01.07 定义信息（数据）和系统所有权。			数据分类准则	APO03.02；APO14.01；BAI02.01；DSS05.02；DSS06.01
			数据安全和控制准则	APO14.04；APO14.10；BAI02.01
			数据完整性程序	APO14.04；BAI02.01；DSS06.01
APO01.08 定义技能和能力目标。			目标技能和能力矩阵	APO07.03
APO01.09 定义并沟通政策和程序。	DSS01.04	环境政策	违规补救措施	MEA01.05
	MEA03.02	已更新的政策、原则、程序和标准		
APO01.10 定义并实施基础设施、服务和应用程序，以支持治理和管理系统。	APO09.01	已确定的为业务提供的 I&T 服务的差距	适当的 I&T 环境计划，包括缺失的 I&T 能力、服务和应用程序	APO02.02；APO02.03
	在 COBIT 外部	I&T 环境评估，包括服务、应用程序和基础设施		

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
APO01.11 管理 I&T 管理系统的持续改进。	**自**	**描述**	**描述**	**至**
	APO01.03	流程能力级别	流程改进机会	所有 APO； 所有 BAI； 所有 DSS； 所有 MEA
	EDM01.03	关于治理有效性和绩效的反馈	流程改进跟踪的绩效目标和指标	MEA01.02
	MEA03.02	已更新的政策、原则、程序和标准	流程能力评估	MEA01.03

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
IT 治理	Skills Framework for the Information Age，第 6 版，2015 年	GOVN
IT 管理	Skills Framework for the Information Age，第 6 版，2015 年	ITMG

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
I&T 管理框架	根据企业目标和其他设计因素建立企业的 I&T 管理系统。 考虑所有组件的详细 I&T 管理政策和原则。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
营造一种业务与 IT 保持一致的内部文化，建立必要的管理目标、结构、流程以及角色和职责，从而以最高效和最有效的方式做出决策和创造价值。		

G. 组件：服务、基础设施和应用程序
• COBIT 和相关产品/工具 • 等效框架和标准

领域：调整、规划和组织 管理目标：APO02 — 妥当管理的战略	焦点领域：COBIT 核心模型

描述

全面了解当前的业务和 I&T 环境、未来发展方向以及营造理想环境所需的举措。确保期望的数字化水平是未来发展方向和 I&T 战略不可或缺的一部分。评估组织当前的数字成熟度并制定路线图来弥补差距。与业务部门一起重新考虑内部运营以及面向客户的活动。确保专注于整个组织的转型过程。利用企业架构构建块、治理组件和组织的生态系统，包括外部提供的服务和相关功能，以实现对战略目标的可靠但灵活和高效的响应。

目的

支持组织的数字化转型战略，并通过递增路线图实现期望的价值。采用 I&T 整体性方法，确保每项举措都与总体战略明确相关。推动组织实现所有方面的变革，从渠道和流程到数据、文化、技能、运营模式和激励机制。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG05 以客户为中心的服务文化 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	AG08 通过集成应用程序和技术来推行和支持业务流程

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG08	a. 执行业务服务或流程的时间 b. 因技术集成问题而延迟或产生额外成本的 I&T 促成的业务计划的数量 c. 因技术集成问题需要延迟或返工的业务流程变更的数量 d. 独立运行和未集成的应用程序或关键基础设施的数量
EG05	a. 客户服务中断的次数 b. 业务利益相关方认为客户服务交付达到议定水平的百分比 c. 客户投诉的数量 d. 客户满意度调查结果的变化趋势		
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比		

A. 组件：流程	
管理实践	**指标示例**
APO02.01 了解企业环境和方向。 了解企业环境（行业驱动因素、相关法规、竞争基础）、当前的运作方式以及期望的数字化水平。	a. I&T 管理层对企业当前的组织和环境的了解水平 b. I&T 管理层对企业目标和方向的知识水平 c. 关键利益相关方对 I&T 及其详细要求的了解水平

活动	能力级别
1. 建立并保持对企业外部环境的了解。	2
2. 建立并保持对当前运作方式的了解，包括运营环境、企业架构（业务、信息、数据、应用和技术领域）、企业文化和面临的挑战。	
3. 建立并保持对企业未来方向的了解，包括企业战略、目的和目标。了解企业期望的数字化水平，可能包括一系列越来越高的目标：从削减成本，强化以客户为中心的服务意识，或通过内部运营的数字化加快产品上市时间，到通过新业务模式（例如平台业务）获得全新的收入流。	
4. 确定关键利益相关方并深入了解他们的要求。	

相关指南（标准、框架、合规性要求）	详细参考
COSO Enterprise Risk Management，2017 年 6 月	7. Strategy and Objective-Setting—Principle 6

管理实践	指标示例
APO02.02 评估企业当前的能力、绩效和数字成熟度。 评估当前 I&T 服务的绩效，并了解当前的业务和 I&T 能力（内部和外部）。评估企业当前的数字成熟度及变革兴趣。	a. 对当前能力感到满意的员工的百分比 b. 业务所有者对投资和利用内外部资产基础来推动关键成功因素感到满意的百分比

活动	能力级别
1. 建立当前业务和 I&T 能力与服务的基准，包括评估外部提供的服务、I&T 治理，以及整个企业的 I&T 相关技能和能力。	2
2. 评估不同维度的数字成熟度（例如，领导层利用技术的能力、可接受的技术风险水平、创新方法、文化和用户的知识水平）。评估变革的意愿。	3

相关指南（标准、框架、合规性要求）	详细参考
COSO Enterprise Risk Management，2017 年 6 月	7. Strategy and Objective-Setting—Principle 6; 9. Review and Revision—Principle 15

管理实践	指标示例
APO02.03 定义数字化能力目标。 基于对企业环境和方向的了解，定义目标 I&T 产品和服务以及所需的能力。考虑参考标准、最佳实践和经过验证的新兴技术。	a. 通过 I&T 目的/目标实现的企业目标的百分比 b. 支持企业战略的 I&T 目标的百分比

活动	能力级别
1. 总结企业环境和方向，并确定企业战略的具体 I&T 方面（例如，流程数字化、实施新技术、支持原有架构、应用新的数字业务模式、开发数字产品组合等）。	2
2. 定义高层面的 I&T 目的和目标，并阐述它们对实现企业目标的贡献。	
3. 详述实现企业目标所需的 I&T 服务和产品。考虑经过验证的新兴技术或创新想法、参考标准、竞争对手业务和 I&T 能力、可比较的良好实践基准，以及新兴的 I&T 服务提供。	3
4. 确定实现定义的 I&T 产品和服务组合所需的 I&T 能力、方法和组织方式。根据业务需求考虑不同的开发方法（敏捷、Scrum、瀑布式、双模式 IT）。考虑每种方法对实现 I&T 目标的帮助。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
APO02.04 执行差距分析。 确定当前环境和目标环境之间的差距，并描述企业架构的高层次变更。	a. 不同企业架构领域所需的高影响力变更的数量 b. 当前环境与良好实践之间的重大差距的数量

活动	能力级别
1. 确定所有差距以及实现目标环境需要进行的变更。	3
2. 描述企业架构的高层次变更（业务、信息、数据、应用和技术领域）。	
3. 考虑所有差距的高层次影响。评估潜在变更对业务和 I&T 运营模式、I&T 研发能力以及 I&T 投资计划的影响。	
4. 考虑潜在变更对业务和 IT 能力、I&T 服务和企业架构的价值，以及未能实现变更将产生的影响。	4
5. 优化目标环境的定义，并制定一份概述目标环境优势的价值综述。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO02.05 定义战略计划和路线图。 与利益相关方合作制定整体数字战略，并制定详细路线图来确定实现目的和目标所需的渐进步骤。任命一位负责人来引领数字化转型并推动业务与 I&T 保持一致，从而确保专注于转型过程。	a. 利益相关方对数字化转型计划的支持程度 b. I&T 战略中自筹资金（且财务效益大于成本）的举措的百分比 c. 企业战略与 I&T 战略和目标的对应程度

活动	能力级别
1. 确定缩小当前环境与目标环境之间的差距所需的举措。将这些举措整合到一致的 I&T 战略中，使 I&T 与业务的各个方面保持一致。	3
2. 制定详细规划图来确定实现 I&T 战略的目的和目标所需的渐进步骤。确保纳入相应的措施，为员工提供新技能培训，支持采用新技术，以及维持整个组织的变革等。	
3. 考虑外部生态系统（企业合作伙伴、供应商、初创企业等），以支持路线图的执行。	
4. 将行动整合成具有明确目标或交付成果的计划和/或项目。为每个项目确定高层次的资源要求、进度、投资/运营预算、风险、变更影响等。	
5. 确定项目之间的依存关系、重叠、协同作用和影响，并确定项目的优先级。	
6. 最终确定路线图，指出项目的相对调度和相互依存关系。	
7. 确保专注于转型过程。任命一位负责人（首席数字官 [CDO] 或其他传统高管角色）来支持数字化转型以及业务与 I&T 之间的一致性。	
8. 获得利益相关方对计划的支持和正式批准。	
9. 将目标转化为可通过指标（什么）和目标（多少）来表示的可衡量成果。确保成果和衡量指标与企业效益相关。	4

相关指南（标准、框架、合规性要求）	详细参考
ISF, The Standard of Good Practice for Information Security 2016	SG2.1 Information Security Strategy
ITIL 第 3 版，2011 年	Service Strategy, 4.1 Strategy management for IT services

A. 组件：流程（续）	
管理实践	**指标示例**
APO02.06 沟通 I&T 战略和方向。 通过与整个企业范围的适当利益相关方和用户沟通，认识和理解 I&T 战略中包含的业务、I&T 目标和方向。	a. I&T 战略沟通计划的更新频率 b. 了解 I&T 战略和方向的利益相关方的百分比

活动	能力级别
1. 制定包含所需信息、目标受众、沟通机制/渠道和时间表的沟通计划。	3
2. 使用可用的媒体和技术来准备能够有效实现计划的沟通工作包。	
3. 建立和维护批准、支持和推动 I&T 战略的网络。	
4. 获取反馈，必要时更新沟通计划和交付。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构																		
关键管理实践	**首席执行官**	**首席信息官**	**首席技术官**	**首席数字官**	**I&T 治理委员会**	**业务流程所有者**	**项目管理办公室**	**数据管理职能部门**	**关系经理**	**架构总监**	**开发总监**	**IT 运营总监**	**IT 行政总监**	**服务经理**	**信息安全经理**	**业务连续性经理**	**隐私官**
APO02.01 了解企业环境和方向。		A	R	R				R	R	R	R	R	R	R	R	R	R
APO02.02 评估企业当前的能力、绩效和数字成熟度。		A	R	R				R		R	R	R	R	R	R	R	R
APO02.03 定义数字化能力目标。		R	R	A		R		R	R	R	R	R	R	R	R	R	R
APO02.04 执行差距分析。		R	R	R	A	R		R		R	R	R	R	R	R	R	R
APO02.05 定义战略计划和路线图。		R	R	R	A	R	R	R		R	R	R	R	R	R	R	R
APO02.06 沟通 I&T 战略和方向。	R	R	R	R	A												

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 38502:2017(E)	5.4 Responsibilities of managers

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	**输入**		**输出**	
APO02.01 了解企业环境和方向。	**自**	**描述**	**描述**	**至**
	APO04.02	关联到业务驱动因素的创新机会	变更的来源和优先级	内部
	EDM04.01	资源和能力分配的指导原则		
	在 COBIT 外部	企业战略和优势、劣势、机会、威胁 (SWOT) 分析		

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
	自	**描述**	**描述**	**至**
APO02.02 评估企业当前的能力、绩效和数字成熟度。	APO06.05	成本优化机会	当前能力存在的相关差距和风险	APO12.01
	APO08.05	潜在改进项目的定义	能力 SWOT 分析	内部
	APO09.01	已确定的为业务提供的IT 服务的差距	当前能力的基准	内部
	APO09.04	改进行动计划和补救措施		
	APO12.01	新出现的风险问题和因素		
	APO12.02	风险分析结果		
	APO12.03	汇总的风险概况，包括风险管理行动的状态		
	APO12.05	旨在降低风险的项目建议		
	BAI04.03	• 已排定优先级的改进 • 性能和容量计划		
	BAI04.05	纠正措施		
	BAI09.01	预期用途审查的结果		
	BAI09.04	• 成本优化审查的结果 • 降低资产成本或创造更高价值的机会		
	EDM04.03	对资源和能力分配及有效性的反馈		
APO02.03 定义数字化能力目标。	APO04.05	• 来自概念验证举措的结果和建议 • 被拒绝举措的分析	建议的企业架构变更	APO03.03
			需要的业务和 IT 能力	内部
			高层次 I&T 相关目标	内部
APO02.04 执行差距分析。	APO04.06	关于使用创新方法的评估	为实现目标能力需要弥补的差距和做出的变更	APO01.03；APO13.02；BAI03.11；EDM04.01
	APO05.01	投资回报预期	目标环境的价值效益说明	BAI03.11
	BAI01.05	计划目标实现情况的监控结果		
	BAI01.06	阶段-关卡审查结果		
	BAI11.09	实施后审查的结果		
	EDM02.02	战略一致性的评估		

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
APO02.05 定义战略计划和路线图。	**自**	**描述**	**描述**	**至**
	APO03.01	• 定义的架构范围 • 架构概念的业务案例和价值主张	I&T 战略和目标	所有 APO； 所有 BAI； 所有 DSS； 所有 MEA
	APO03.02	信息架构模型	战略路线图	APO01.01； APO03.01； APO08.01； EDM02.01； EDM02.02
	APO03.03	过渡架构	战略举措的定义	EDM02.01
	APO05.01	资金选择	风险评估举措	EDM02.01； APO12.01
	APO06.02	预算分配		
	APO06.03	I&T 预算		
	BAI09.05	调整许可证数量和分配情况的行动计划		
	DSS04.02	获得批准的战略方案		
	EDM02.01	战略和目标反馈		
	EDM04.01	已批准的资源计划		
	EDM04.03	解决资源管理偏离的补救措施		
APO02.06 沟通 I&T 战略和方向。	EDM04.02	资源配置战略的沟通	沟通工作包	所有 APO； 所有 BAI； 所有 DSS； 所有 MEA
			沟通计划	内部

相关指南（标准、框架、合规性要求）	详细参考
ITIL 第 3 版，2011 年	Service strategy, 3.9 Service strategy inputs and outputs

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
业务计划制定	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	A. Plan—A.3. Business Plan Development
新兴技术的监控	Skills Framework for the Information Age，第 6 版，2015 年	EMRG
I&T 战略和规划	Skills Framework for the Information Age，第 6 版，2015 年	ITSP
战略一致性	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	A. Plan—A.1. IS and Business Strategy Alignment

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
I&T 服务战略原则	有关详细信息，请参阅相关指南。	ITIL 第 3 版，2011 年	Service Strategy，3. Service strategy principles
I&T 战略政策和原则	全面了解当前的业务和 I&T 环境、战略方向以及过渡到理想环境所需的举措。确保业务和 I&T 战略反映了数字化目标水平。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
建立适合整体业务战略的文化和基本价值观（即以客户为中心、以创新为导向、以产品为基础）。设法提高流程速度并引入支持流程的文化和行为，从而实现更快的发展速度。可以从改变习惯开始，例如更频繁地召开战略领导会议或实现某些活动的自动化。 在当前的数字业务模式、生态系统和干扰的背景下，对很多组织来说，在战略中优先考虑数字化转型至关重要。建立勇于打破现状和探索新工作方式的文化（例如，投资自动化以快速响应客户；开发先进的报告和分析功能以解读客户需求；构建创新的界面以收集客户数据；创建通过所有相关渠道交付内容和服务的机制）。	The Scaled Agile Framework for Lean Enterprises	可帮助组织以最短的可持续交付周期交付新产品和解决方案的可配置性框架（所有章节）

G. 组件：服务、基础设施和应用程序
• 客户分析 • 行业基准 • 绩效衡量系统（例如平衡计分卡、技能管理工具） • 技术观察服务和工具

领域：调整、规划和组织 管理目标：APO03 — 妥当管理的企业架构	焦点领域：COBIT 核心模型

描述

建立通用架构，包括业务流程、信息、数据、应用和技术架构层。根据企业和 I&T 战略，建立描述基准架构和目标架构的关键模型和实践。定义有关分类、标准、指南、程序、模板和工具的要求并提供这些组件之间的关联。改进一致性、提高敏捷性、改善信息质量并通过重用构建块组件等举措实现潜在的成本节约。

目的

表示不同的构建区块，它们构成企业及其相互关系以及指导设计与发展演变的原则，促进标准、快速及有效地交付运营和战略目标。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG05 以客户为中心的服务文化 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	• AG06 将业务需求转化为可运作的解决方案的敏捷性 • AG08 通过集成应用程序和技术来推行和支持业务流程

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG06	a. 业务高管对 I&T 响应新需求的满意度水平 b. 新的 I&T 相关服务和应用程序的平均上市时间 c. 将战略 I&T 目标转化为议定的已批准举措所需的平均时间 d. 受最新基础设施和应用支持的关键业务流程的数量
EG05	a. 客户服务中断的次数 b. 业务利益相关方认为客户服务交付达到议定水平的百分比 c. 客户投诉的数量 d. 客户满意度调查结果的变化趋势	AG08	a. 执行业务服务或流程的时间 b. 因技术集成问题而延迟或产生额外成本的 I&T 促成的业务计划的数量 c. 因技术集成问题需要延迟或返工的业务流程变更的数量 d. 独立运行和未集成的应用程序或关键基础设施的数量
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比		

A. 组件：流程

管理实践	指标示例
APO03.01 制定企业架构愿景。 架构愿景提供了基准架构和目标架构的第一次高层次描述，涵盖业务、信息、数据、应用和技术领域。架构愿景为发起人提供了关键工具，帮助在企业内部积极介绍建议功能的好处，以便说服利益相关方接受。架构愿景描述了新能力（与 I&T 战略和目标保持一致）将如何满足企业目标和战略目标，并在实施过程中消除利益相关方的顾虑。	a. 架构客户的反馈水平 b. 基准架构和目标架构涵盖业务、信息、数据、应用和技术领域的程度以及更新频率

A. 组件：流程（续）	
活动	**能力级别**
1. 识别关键利益相关方及其顾虑/目标。确定待解决的关键企业需求以及为满足利益相关方需求而应建立的架构视图。	2
2. 识别企业目标和战略驱动因素。确定必须解决的约束，包括整个企业和项目特定的约束（例如时间、进度、资源等）。	
3. 使架构目标与战略计划优先级保持一致。	
4. 了解企业能力和目标，然后确定实现这些目标的方案。	
5. 评估企业是否准备好变更。	
6. 定义基准架构和目标架构的范围。列举范围内和范围外的项目。（无需以相同的详细程度描述基准架构和目标架构。）	
7. 了解企业当前的战略目的和目标。在战略计划流程中开展工作，确保利用 I&T 相关的企业架构机会来制定战略计划。	
8. 基于利益相关方的顾虑、业务能力要求、范围、约束和原则来创建架构愿景（即高层次的基准架构和目标架构）。	
9. 确认并详述架构原则，包括企业原则。确保所有现有定义都是最新的。澄清任何含糊不清之处。	3
10. 识别与架构愿景相关的企业变更风险。评估初始风险级别（例如关键、边际或可忽略不计）。为每项重大风险制定缓解策略。	
11. 开发企业架构概念业务案例并概述架构工作的计划和说明。获得批准，启动与企业战略一致并与之整合的项目。	
12. 定义目标架构的价值主张、目标和指标。	4

相关指南（标准、框架、合规性要求）	**详细参考**
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.15 Program management (PM-7)
The Open Group Standard TOGAF，第 9.2 版，2018 年	6. Phase A: Architecture Vision
管理实践	**指标示例**
APO03.02 定义参考架构。 参考架构描述了业务、信息、数据、应用和技术领域的当前和目标架构。	a. 领域和/或联合架构的最后更新日期 b. 已应用和授权的架构标准和基准的例外情况的数量

活动	**能力级别**
1. 维护包含标准、可重用组件、建模构件、关系、依存关系和视图的架构贮存库，使架构的组织和维护保持一致。	3
2. 从架构贮存库中选择参考视角，以便架构师能够证明如何在架构中解决利益相关方的顾虑。	
3. 为每个视角选择支持必要的特定视图所需的模型。使用选定的工具或方法以及合适的分解水平。	
4. 使用支持目标架构所需的范围和详细程度编写基准架构领域说明，并尽可能识别架构贮存库中的相关架构构建块。	
5. 将流程架构模型作为基准和目标领域说明的一部分进行维护。实现流程描述和文档的标准化。定义流程决策者、流程所有者、流程用户、流程团队以及应参与的任何其他流程利益相关方的角色和责任。	
6. 以符合企业战略的方式，将信息架构模型作为基准和目标领域说明的一部分进行维护，从而以最佳方式获取数据、存储数据和使用数据来支持决策。	
7. 验证架构模型的内部一致性和准确性。执行基准与目标的差距分析。确定差距的优先级，并定义必须为目标架构开发的新组件或修改后的组件。解决目标架构中的不兼容、不一致或冲突问题。	
8. 开展正式的利益相关方审查，根据架构项目的本意和架构工作说明来审查建议的架构。	
9. 最终确定业务、信息、数据、应用和技术领域的架构。创建架构定义文档。	

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI 数据管理成熟度模型，2014 年	Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
ITIL 第 3 版，2011 年	Service Strategy, 5.4 IT service strategy and enterprise architecture
美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	3.1 Preparation (Task 9)
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.5 Configuration management (CM-8)
The Open Group Standard TOGAF，第 9.2 版，2018 年	7. Phase B: Business Architecture; 8. Phase C: Information Systems Architectures; 9. Phase C: Information Systems Architectures Data Architecture; 10. Phase C: Information Systems Architectures Application Architecture; 11. Phase D: Technology Architecture
管理实践	**指标示例**
APO03.03 选择机会和解决方案。 从业务和技术角度合理解释基准架构与目标架构之间的差距，并将其合理分组，归入项目工作包。将项目与任何相关的 I&T 促成的投资计划相结合，确保架构举措作为整个企业变更的一部分，与这些举措保持一致并且能够起到促进作用。与企业内业务和 IT 领域的关键利益相关方合作，评估企业转型的就绪情况，并识别机会、解决方案和所有实施限制。	a. 已在企业、信息、数据、应用和技术架构领域的模型中确定的差距的数量 b. 业务和 IT 领域的关键利益相关方中参与了评估企业转型的就绪情况以及识别机会、解决方案和所有实施限制的百分比

活动	**能力级别**
1. 确定并确认关键的企业变更属性。考虑企业的文化及其对架构实施的潜在影响，以及企业的过渡能力。	3
2. 确定任何会限制实施顺序的企业驱动因素，包括审查企业和业务线的战略和业务计划。考虑企业当前的架构成熟度。	
3. 审查并合并基准架构与目标架构之间的差距分析结果。评估对潜在解决方案、机会、相互依存关系以及与当前 I&T 促成的计划的一致性的影响。	
4. 评估要求、差距、解决方案和其他因素，确定最少的一系列职能要求，将其整合到工作包中可以更高效和有效地实施目标架构。	
5. 核对合并的要求与潜在的解决方案。	
6. 优化初始的依存关系，并识别对实施和迁移计划的限制。编制一份依存性分析报告。	
7. 确认企业是否准备好转型，以及与企业转型相关的风险。	
8. 制定高层次的实施和迁移战略。根据企业整体战略、目标和时间表实施目标架构（并安排任何过渡架构）。	
9. 确定主要工作包，并将其分组到与企业战略实施方向和方法有关的一系列相关计划和项目中。	
10. 如果实现目标架构所需的变更范围必须使用递增方法，应开发过渡架构。	

相关指南（标准、框架、合规性要求）	**详细参考**
CMMI 数据管理成熟度模型，2014 年	Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
The Open Group Standard TOGAF，第 9.2 版，2018 年	12. Phase E: Opportunities and Solutions

A. 组件：流程（续）	
管理实践	**指标示例**
APO03.04 定义架构实施。 建立与计划和项目组合一致的可行实施和迁移计划。确保紧密协调计划以创造价值，并提供必要的资源来完成必要的工作。	a. 明确定义的架构实施治理要求 b. 了解架构实施与迁移的利益相关方的百分比

活动	能力级别
1. 在计划及项目规划期间建立实施和迁移计划所需的项目。确保计划满足相关决策者的要求。	3
2. 确认过渡架构的增量和阶段。更新架构定义文档。	
3. 定义并完成架构实施和迁移计划，包括相关的治理要求。将计划、活动和依存关系整合到计划及项目规划中。	
4. 向利益相关方沟通已确定的架构路线图。向利益相关方沟通目标架构的定义、架构准则和原则，以及服务组合等。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
The Open Group Standard TOGAF，第 9.2 版，2018 年	13. Phase F: Migration Planning

管理实践	指标示例
APO03.05 提供企业架构服务。 在企业内提供企业架构服务，包括指导和监控项目的实施，通过架构合同正式规定工作方式，以及衡量和沟通架构的价值与合规性监控。	a. 客户对架构服务的反馈水平 b. 采用框架和方法来复用已定义组件的项目的百分比 c. 使用企业架构服务的项目的百分比 d. 可追溯到架构参与（例如，通过复用来降低成本）的已实现项目效益

活动	能力级别
1. 确认范围和优先级，并为解决方案的开发和部署（例如，通过采用面向服务的架构）提供指南。	3
2. 采用关于架构原则、模型和构建块的建议和专业知识来管理企业架构要求并支持业务和 IT。保证新的实施（以及当前架构的变更）与企业架构原则和要求保持一致。	
3. 管理企业架构服务组合，并确保其与战略目标和解决方案开发保持一致。	
4. 确定企业架构优先级。使优先级与价值驱动因素保持一致。定义和收集价值指标，以及衡量和沟通企业架构的价值。	4
5. 建立技术论坛来提供架构准则和项目建议，并指导技术的选择。衡量标准和准则的遵从情况，包括对外部要求的遵从情况和内部业务相关性。	5

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Platform and Architecture—Architectural Standards
ITIL 第 3 版，2011 年	Service Design, 3.9 Service Oriented Architecture
The Open Group Standard TOGAF，第 9.2 版，2018 年	14. Phase G: Implementation Governance; 15. Phase H: Architecture Change Management

B. 组件：组织结构								
关键管理实践	首席运营官	首席信息官	首席技术官	首席数字官	I&T 治理委员会	架构委员会	数据管理职能部门	架构总监
APO03.01 制定企业架构愿景。		R	R	R	R	A	R	R
APO03.02 定义参考架构。		R	R	R	R	A	R	R
APO03.03 选择机会和解决方案。		R	R	R	R	A	R	R
APO03.04 定义架构实施。	R	R	R	R	R	A	R	R
APO03.05 提供企业架构服务。	R	R	R	R	R	A		R

相关指南（标准、框架、合规性要求）	详细参考
The Open Group Standard TOGAF，第 9.2 版，2018 年	41. Architecture Board

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
APO03.01 制定企业架构愿景。	APO02.05	战略路线图	定义的架构范围	APO02.05
	EDM04.01	企业架构的指导原则	架构概念的业务案例和价值主张	APO02.05；APO05.02
	在 COBIT 外部	企业战略	架构原则	BAI02.01；BAI03.01；BAI03.02
APO03.02 定义参考架构。	APO01.04	• 组织结构和职能的定义 • 企业运营准则	流程架构模型	APO01.04
	APO01.06	• IT 组织方案的评估 • 已定义的 IT 职能运营设置	信息架构模型	APO02.05；APO14.03；BAI02.01；BAI03.02；DSS05.03；DSS05.04；DSS05.06

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
APO03.02 定义参考架构。*（续）*	**自**	**描述**	**描述**	**至**
	APO01.07	数据分类准则	基准指标领域说明和架构定义	APO13.02；BAI02.01；BAI03.01；BAI03.02；BAI03.12
	APO14.01	数据管理战略		
	APO14.03	元数据文档		
	在 COBIT 外部	企业战略		
APO03.03 选择机会和解决方案。	APO02.03	建议的企业架构变更	过渡架构	APO02.05
	在 COBIT 外部	• 企业驱动因素 • 企业战略		
APO03.04 定义架构实施。			实施阶段的描述	BAI01.01；BAI01.02；BAI11.01
			架构治理要求	BAI01.01；BAI11.01
			资源要求	BAI01.02
APO03.05 提供企业架构服务。			解决方案开发指南	BAI02.01；BAI02.02；BAI03.02；BAI03.12

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-37，修订版 2，2017 年 9 月	3.1 Preparation (Task 9): Inputs and Outputs
The Open Group Standard TOGAF，第 9.2 版，2018 年	6. Phase A: Architecture Vision: Inputs and Outputs; 7. Phase B: Business Architecture: Inputs and Outputs; 9. Phase C: Information Systems Architectures Data Architecture: Inputs and Outputs; 10. Information Systems Architectures Application Architecture: Inputs and Outputs; 11. Phase D: Technology Architecture: Inputs and Outputs; 12. Phase E: Opportunities and Solutions: Inputs and Outputs; 13. Phase F: Migration Planning: Inputs and Outputs; 14. Phase G: Implementation Governance: Inputs and Outputs; 15. Phase H: Architecture Change Management: Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
架构设计	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	A. Plan—A.5. Architecture Design
数据分析	Skills Framework for the Information Age，第 6 版，2015 年	DTAN
企业和业务架构	Skills Framework for the Information Age，第 6 版，2015 年	STPL
产品/服务规划	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	A. Plan—A.4. Product/Service Planning
解决方案架构	Skills Framework for the Information Age，第 6 版，2015 年	ARCH

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
架构原则	阐明一般原则，用于规定以下方面的规则和 “20. Architecture Principles” 准则：架构流程、程序、层面以及 I&T 资源和资产的总体使用和互连。概述加强决策能力的架构原则。确保当前架构和目标架构与企业目标和战略保持一致。	The Open Group Standard TOGAF，第 9.2 版，2018 年	20. Architecture Principles

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
营造一种环境，使管理层了解与业务目的和目标相关的架构需求。推动整个组织（不仅仅是企业架构师）有效地践行企业架构。确保采用整体方法，实现组件间更加无缝的衔接（例如，取消专门的应用程序专家团队）。		

G. 组件：服务、基础设施和应用程序
架构贮存库

领域：调整、规划和组织 管理目标：APO04 — 妥当管理的创新	焦点领域：COBIT 核心模型

描述

保持对 I&T 及其相关服务趋势的意识并监控新兴技术趋势。积极发现创新机会，并计划如何从与业务需求和既定 I&T 战略相关的创新中获益。分析通过新兴技术、服务或 I&T 促成的业务创新、现有的成熟技术，以及业务和 IT 流程创新可以创造哪些业务创新或改进的机会。影响战略计划和企业架构决策。

目的

利用 I&T 发展和新兴技术来获取竞争优势、推动业务创新、提高客户体验以及改善运营效率和效果。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG13 产品和业务创新	• AG06 将业务需求转化为可运作的解决方案的敏捷性 • AG13 业务创新的知识、专业技能和举措

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG06	a. 业务高管对 I&T 响应新需求的满意度水平 b. 新的 I&T 相关服务和应用程序的平均上市时间 c. 将战略 I&T 目标转化为议定的已批准举措所需的平均时间 d. 受最新基础设施和应用支持的关键业务流程的数量
EG13	a. 对业务创新机会的认识和理解水平 b. 利益相关方对产品以及创新专长和想法的满意度 c. 源自创新想法的已批准产品和服务举措的数量	AG13	a. 业务高管对 I&T 创新可能性的认识和理解水平 b. 源自 I&T 创新想法的已批准举措的数量 c. 获得认可/奖励的创新推动者的数量

A. 组件：流程

管理实践	指标示例
APO04.01 营造适宜创新的环境。 营造适宜创新的环境，考虑采用诸如文化、奖励、协作、技术论坛，以及促进和获取员工想法的机制。	a. 企业利益相关方对 I&T 创新的认知和反馈 b. 将创新或新兴技术相关的目标纳入相关员工的绩效考核目标

活动	能力级别
1. 制定创新计划，其中包括风险偏好、创新举措的预算建议和创新目标。	2
2. 提供可以成为创新治理组件的基础设施（例如增强不同地理位置和/或部门之间合作的协作工具）。	
3. 维护一项促使员工提交创新想法的计划，并建立相应的决策结构以评估和向前推进这些想法。	3
4. 鼓励客户、供应商和业务合作伙伴提出创新想法。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
APO04.02 保持对企业环境的了解。 与相应的利益相关方合作，以了解他们面临的挑战。保持对企业战略、竞争环境和其他制约的充分了解，以识别新技术带来的机遇。	a. 与企业目标明确关联的已实施举措的百分比 b. 由已识别的新技术带来的机遇的百分比

活动	能力级别
1. 保持对行业和业务驱动因素、企业和 I&T 战略、企业运营和当前挑战的了解。运用这种了解来识别可能增加价值的技术和创新 I&T。	2
2. 定期与业务部门、单位和/或其他利益相关方实体召开会议，以了解新兴技术或 I&T 创新可以创造机会的当前业务问题、流程瓶颈或其他制约。	3
3. 了解创新和新技术的企业投资参数，以制定适当的战略。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO04.03 监控和审视技术环境。 建立技术跟踪流程以对企业的外部环境进行系统化的监控和审视，确定有可能创造价值的新兴技术（例如实现企业战略、优化成本、避免淘汰以及更好地推行企业和 I&T 流程）。监控市场、竞争格局、行业领域以及法律与法规趋势，以便能够在企业环境中分析新兴技术或创新思路。	a. 为识别创新想法和趋势而开展的环境研究和审视的频率 b. 对通过监控市场、竞争格局、行业领域以及法律与法规趋势来分析企业环境中的新兴技术或创新思路的工作感到满意的利益相关方的百分比

活动	能力级别
1. 了解企业对技术创新的偏好和潜力。聚焦于发现最适宜的技术创新。	2
2. 建立技术跟踪流程，以监控和审视外部环境，包括合适的　　、期刊和会议，以发现新兴技术及其对企业的潜在价值。	
3. 必要时咨询第三方专家，以确认研究结果或了解有关新兴技术的信息。	
4. 获取员工的 I&T 创新想法并评估实施的可能性。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO04.04 评估新兴技术和创新想法的潜力。 分析已识别的新兴技术和/或其他 I&T 创新建议以了解它们的业务潜力。与利益相关方合作验证对新技术与创新潜力的假设。	a. 实现预期效益的已实施举措的百分比 b. 成功执行的旨在测试新兴技术或其他创新想法的概念验证举措的百分比

活动	能力级别
1. 根据企业战略和 I&T 战略评估已确定的技术，考虑达到成熟所需的时间、固有风险（包括潜在法律影响）、与企业架构的契合度以及价值潜力等多个方面。	2
2. 确定可能需要通过概念验证举措解决或验证的任何问题。	3
3. 划定概念验证举措的范围，包括理想成果、所需预算、时间期限以及责任。	
4. 获取对概念验证举措的批准。	
5. 执行概念验证举措以测试新兴技术或其他创新想法。识别问题，并根据可行性和潜在投资回报率确定是否应考虑实施或推行。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
APO04.05 建议适当的进一步举措。 评估并监控概念验证举措的结果，如果顺利，形成有关进一步举措的建议。获得利益相关方支持。	a. 已评估并被批准进一步推行的概念验证举措的数量 b. 已在实际投资中运用的概念验证举措的数量

活动	能力级别
1. 记录概念验证结果，包括有关趋势和创新计划的指导和建议。	3
2. 将切实可行的创新机会传达到 I&T 战略和企业架构流程。	
3. 分析并沟通概念验证举措被拒绝的原因。	
4. 跟进概念验证举措以衡量实际投资。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO04.06 监控创新的实施与使用。 监控新兴技术和创新在采纳、集成及完整经济生命周期期间的实施与使用，确保实现预期效益并总结经验教训。	a. 创新带来的市场份额或竞争力的增加 b. 获取的可供未来使用的经验教训和改进机会的数量

活动	能力级别
1. 获取经验教训和改进机会。	3
2. 确保创新举措与企业战略和 I&T 战略保持一致。持续监控一致性。根据需要调整创新计划。	
3. 评估作为 I&T 战略和企业架构开发的一部分实施的新技术或 I&T 创新。在计划管理期间评估举措的采用情况。	4
4. 确定和评估创新的潜在价值。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构														
关键管理实践	**执行委员会**	**首席信息官**	**首席技术官**	**首席数字官**	**业务流程所有者**	**数据管理职能部门**	**人力资源总监**	**关系经理**	**架构总监**	**开发总监**	**IT 运营总监**	**服务经理**	**信息安全经理**
APO04.01 营造适宜创新的环境。	A	R	R	R	R	R	R		R	R	R	R	R
APO04.02 保持对企业环境的了解。	A	R	R	R	R	R		R	R	R	R	R	R
APO04.03 监控和审视技术环境。	A	R	R	R	R	R			R	R	R	R	R
APO04.04 评估新兴技术和创新想法的潜力。	A	R	R	R	R	R			R	R	R	R	R
APO04.05 建议适当的进一步举措。	A	R	R	R	R	R			R	R	R	R	R
APO04.06 监控创新的实施与使用。	A	R	R	R	R	R			R	R	R	R	R

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
APO04.01 营造适宜创新的环境。	自	描述	描述	至
	EDM03.01	风险偏好的指导准则	认可与奖励计划	APO07.04
			创新计划	内部
APO04.02 保持对企业环境的了解。	在 COBIT 外部	企业战略和优势、劣势、机会、威胁 (SWOT) 分析	关联到业务驱动因素的创新机会	APO02.01
APO04.03 监控和审视技术环境。	在 COBIT 外部	新兴技术	创新可能性的研究分析	BAI03.01
APO04.04 评估新兴技术和创新想法的潜力。			概念验证范围和业务案例大纲	APO05.02；APO06.02
			创新想法的评估	BAI03.01
			概念验证举措的测试结果	内部
APO04.05 建议适当的进一步举措。			被拒绝举措的分析	APO02.03；BAI03.08
			来自概念验证举措的结果和建议	APO02.03；BAI03.09
APO04.06 监控创新的实施与使用。			关于使用创新方法的评估	APO02.04；BAI03.02
			创新效益的评估	APO05.03
			调整的创新计划	内部
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
业务计划制定	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	A. Plan—A.3. Business Plan Development
新兴技术的监控	Skills Framework for the Information Age，第 6 版，2015 年	EMRG
实施创新	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	A. Plan—A.9. Innovating
创新	Skills Framework for the Information Age，第 6 版，2015 年	INOV
研究	Skills Framework for the Information Age，第 6 版，2015 年	RSCH
技术趋势监控	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	A. Plan—A.7. Technology Trend Monitoring

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
创新原则	定义一般原则，确保在定义新的战略目标和决策时充分评估新的/创新的想法。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
通过维护相关 HR 举措来营造适宜创新的环境，这些举措如创新认可和奖励计划、适当轮岗以及自由支配的实验创新时间。确保整个组织就举措开展密切的合作与协调。		

G. 组件：服务、基础设施和应用程序
• 协作平台 • 行业基准 • 技术观察服务和工具

领域：调整、规划和组织 管理目标：APO05 — 妥当管理的组合	焦点领域：COBIT 核心模型

描述

执行设定的战略投资方向，确保与企业的架构愿景和 I&T 路线图保持一致。考虑不同类别的投资以及资源和资金限制。根据与战略目标、企业效益和风险保持一致性的要求，在资源和资金限制下，评估、排序和权衡计划和服务。将选择的计划迁移到有效的产品或服务组合中执行。监控整个产品、服务和计划组合的绩效，根据计划、产品或服务绩效或不断变化的企业优先级进行必要的调整。

目的

优化总体计划组合的绩效，以应对个别计划、产品和服务的绩效以及不断变化的企业优先级和需求。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	• AG03 通过 I&T 促成的投资和服务组合所实现的效益 • AG05 提供符合业务需求的 I&T 服务
企业目标的指标示例	**一致性目标的指标示例**
EG01 a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG03 a. 达到或超过业务案例宣称效益的 I&T 促成的投资的百分比 b. 实现预期效益（如服务水平协议所述）的 I&T 服务的百分比
EG08 a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度	AG05 a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG12 a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比	

A. 组件：流程

管理实践	指标示例
APO05.01 确定资金可用性和来源。 确定潜在的资金来源、不同的资金选择，以及资金来源对投资回报预期的影响。	a. 已分配资金与已使用资金的比率 b. 留存收益与已分配资金的比率

活动	能力级别
1. 了解当前的资金可用性和承诺、当前已批准的费用，以及到目前为止的实际开销。	2
2. 确定为 I&T 促成的投资获取额外资金的方案，包括内部和外部来源。	
3. 确定资金来源对投资回报预期的影响。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
APO05.02 评估和选择要资助的计划。 基于总体投资组合要求、I&T 战略计划和路线图，评估计划业务案例和确定其优先级，并决定投资方案。分配资金和启动计划。	a. I&T 项目组合中可直接追溯到 I&T 战略的项目的百分比 b. 参与评估和优先级确定流程的业务部门的百分比

活动	能力级别
1. 根据投资组合类别识别与分类投资机会。指定预期的企业成果、实现预期成果所需的举措、高层次成本、依存关系和风险。指定衡量成果、成本和风险的方法。	2
2. 对所有计划业务案例进行详细评估。评估战略一致性、企业效益、风险和资源可用性。	3
3. 评估增加潜在计划（包括其他计划可能需要的变更）对总体投资组合的影响。	
4. 决定应将哪些候选计划移到有效投资组合中。决定被拒绝的计划是否应留待将来考虑或为其提供一些种子资金，以确定业务案例能否改进或丢弃。	
5. 为每个选定计划的完整经济生命周期确定所需的里程碑。按照每个里程碑分配和储备总计划资金。将计划移到有效的投资组合中。	
6. 建立沟通组合的成本、效益和风险相关方面的程序，以便在预算优先级确定、成本管理和效益管理流程中加以考虑。	

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 1.2.3 Relationship of project, program, portfolio and operations management

管理实践	指标示例
APO05.03 监控、优化和报告投资组合绩效。 定期监控和优化投资组合和单个计划在整个投资生命周期中的绩效。确保持续跟进投资组合与 I&T 战略的一致性。	a. I&T 战略中举措的投资回报率趋势 b. 对投资组合监控报告的满意度水平 c. 与企业业务要求保持一致的计划的百分比

活动	能力级别
1. 定期审查组合以确定和利用协同作用，消除计划之间的重复内容，并确定和降低风险。	3
2. 发生变更时，重新评估组合并重新排定其优先级，以确保组合与业务和 I&T 战略保持一致。维护目标投资组合，以优化投资组合的总体价值。可以变更、推迟或终止现有计划并启动新计划，以重新平衡和优化投资组合。	
3. 调整企业目标、预测、预算和监控的程度（如果需要），以反映有效投资组合中的计划所产生的费用和实现的企业效益。分摊计划支出。建立灵活的预算流程，使有前景的项目能够获得资源以迅速扩展。	
4. 制定指标来衡量 I&T 对企业的贡献。建立适当的绩效目标，反映需要达成的 I&T 目标和企业能力目标。在外部专家的指导下使用基准指标数据制定指标。	4
5. 将准确的投资组合绩效信息提供给所有利益相关方。	
6. 提供报告供高级管理层审查企业既定目标的进展情况，同时陈述仍需哪些花费以及在给定的时间范围内完成哪些工作。	
7. 定期绩效监控应涵盖以下信息：实现了哪些计划目标、控制了哪些风险、具备了哪些能力、获得了哪些交付成果，以及实现了哪些绩效目标。	
8. 确定预算与实际开销的偏差，以及预期的投资 ROI。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
APO05.04 维护组合。 维护投资计划和项目、I&T 产品和服务以及 I&T 资产的组合。	a. 已完成的计划和项目的数量 b. 距离上次更新服务组合的时间

活动	**能力级别**
1. 创建并维护 I&T 促成的投资计划、I&T 服务和 I&T 资产的组合，形成当前 I&T 预算的基础，并支持 I&T 战术和战略计划。	3
2. 与服务交付经理合作维护服务组合。与运营经理、产品经理和架构师合作维护资产组合。排定组合的优先级以支持投资决策。	
3. 已实现期望的企业效益，或依据计划设定的价值标准明显无法实现期望的价值时，从有效投资组合中删除计划。	

相关指南（标准、框架、合规性要求）	**详细参考**
ITIL 第 3 版，2011 年	Service Strategy，4.2 Service portfolio management

管理实践	**指标示例**
APO05.05 管理效益实现。 基于商定的和当前的业务案例，监控提供和维护适当的 I&T 产品、服务和能力的效益。	a. 反映在相关 I&T 组合中的投资计划变更的百分比 b. 利益相关方对以下工作感到满意的百分比：基于商定的和当前的业务案例，监控提供和维护适当的 I&T 服务和能力的效益

活动	**能力级别**
1. 使用商定的指标跟踪以下方面：效益如何实现；它们在计划和项目的整个生命周期中如何演变；I&T 产品和服务如何交付这些效益；以及它们与内部和行业基准的比较结果。与利益相关方沟通结果。	4
2. 当实现的效益与预期效益差距较大时，采取纠正措施。将新举措更新到业务案例，并根据需要实施业务流程和服务改进。	5
3. 考虑从外部专家、行业领导者和比较基准检测数据获得指导，以测试并改进衡量指标和目标。	

相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	

B. 组件：组织结构										
关键管理实践	首席财务官	首席信息官	首席技术官	首席数字官	I&T 治理委员会	业务流程所有者	组合经理	计划经理	项目管理办公室
APO05.01 确定资金可用性和来源。	R	R			A		R		
APO05.02 评估和选择要资助的计划。	R	R	R	R	A		R	R	
APO05.03 监控、优化和报告投资组合绩效。		R	R	R	A		R	R	
APO05.04 维护组合。		R	R	R	A		R	R	R
APO05.05 管理效益实现。	R	R	R	R	A	R	R	R	
相关指南（标准、框架、合规性要求）	**详细参考**								
本组件没有相关指南									

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
APO05.01 确定资金可用性和来源。	**自**	**描述**	**描述**	**至**
			投资回报预期	APO02.04；APO06.02；BAI01.06；EDM02.02
			资金选择	APO02.05

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
APO05.02 评估和选择要资助的计划。	**自**	**描述**	**描述**	**至**
	APO03.01	架构概念的业务案例和价值主张	计划业务案例	APO06.02；BAI01.02
	APO04.04	概念验证范围和业务案例大纲	业务案例评估	APO06.02；BAI01.06
	APO06.02	• 预算分配 • 确定 I&T 举措的优先级和等级	包含 ROI 里程碑的精选计划	BAI01.04；EDM02.02
	APO06.03	• IT 预算 • 预算沟通		
	APO09.01	已确定的为业务提供的IT 服务的差距		
	APO09.03	服务水平协议 (SLA)		
	APO13.02	信息安全业务案例		
	BAI01.02	• 计划的效益实现规划 • 计划概念业务案例 • 计划授权和概要		
	EDM02.02	• 战略一致性的评估 • 投资和服务组合的评估		
	EDM02.03	投资类型和标准		
APO05.03 监控、优化和报告投资组合绩效。	APO04.06	创新效益的评估	投资组合绩效报告	APO09.04；BAI01.06；EDM02.03；EDM02.04；MEA01.03
	BAI01.06	阶段-关卡审查结果		
	EDM02.02	投资和服务组合的评估		
	EDM02.04	• 组合和计划绩效的反馈 • 改进实现价值的措施		
APO05.04 维护组合。	BAI01.09	计划终止和持续责任的沟通	更新的计划、服务和资产组合	APO09.02；BAI01.01
	BAI03.11	更新的服务组合		
APO05.05 管理效益实现。	BAI01.04	计划预算和效益登记表	改进效益实现的纠正措施	APO09.04；BAI01.06
	BAI01.05	效益实现的监控结果	效益结果和相关沟通	APO09.04；BAI01.06；EDM02.02
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
效益管理	Skills Framework for the Information Age，第 6 版，2015 年	BENM
组合管理	Skills Framework for the Information Age，第 6 版，2015 年	POMG
产品/服务规划	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	A. Plan—A.4. Product/Service Planning

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
组合原则	定义总体原则，确保选择正确且多元化的计划和项目来实现 I&T 战略；考虑与业务战略、适当的投资组合等保持一致。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
推动 I&T 投资的系统化管理；客观地衡量和评估投资方案。		
为提高速度和敏捷性，确保领导者果断评估有效的投资组合。如果原型无法正常运行，领导者必须果断地结束项目、吸取经验教训并继续前进。快速将其他资源投入到成功的项目中，以适当地扩展项目。		

G. 组件：服务、基础设施和应用程序
组合/投资管理工具

领域：调整、规划和组织 管理目标：APO06 — 妥当管理的预算和成本	焦点领域：COBIT 核心模型

描述

使用正式的预算实践和公平公正的企业成本分配系统来管理业务和 IT 职能部门的 I&T 相关财务活动，包括预算、成本和效益管理以及支出的优先级确定。咨询利益相关方，识别和控制 I&T 战略及战术计划背景下的总成本和效益。必要时采取纠正措施。

目的

促进 IT 与企业利益相关方之间的合作伙伴关系，有效和高效地使用 I&T 相关资源，在解决方案和服务的成本与业务价值方面保持透明并采取问责制。使企业能够就 I&T 解决方案和服务的使用做出明智的决策。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG04 财务信息的质量 • EG07 管理信息的质量 • EG08 内部业务流程功能的优化 • EG09 业务流程成本的优化 • EG12 妥当管理的数字化转型计划	• AG04 技术相关财务信息的质量 • AG09 在预算内按时交付计划且满足要求和质量标准

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG04	a. 有关 I&T 财务信息的透明度、了解度和准确性水平的关键利益相关方满意度 b. 已定义运营成本和预期效益并获得批准的 I&T 服务的百分比
EG04	a. 有关企业财务信息的透明度、了解度和准确性的关键利益相关方满意度调查 b. 不遵守财务相关法规的成本	AG09	a. 在预算内按时交付的计划/项目的数量 b. 因质量缺陷需要重大返工的计划的数量 c. 对计划/项目质量满意的利益相关方的百分比
EG07	a. 董事会和执行管理层对决策信息的满意度 b. 基于不准确信息的错误业务决策所导致的事故数量 c. 为有效业务决策提供支持性信息所花的时间 d. 管理信息的及时性		
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		
EG09	a. 成本与达到的服务水平的比率 b. 董事会和执行管理层对业务流程成本的满意度		
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比		

A. 组件：流程	
管理实践	**指标示例**
APO06.01 管理财务和会计。 作为企业财务系统和会计科目表不可或缺的一部分，建立并维护涵盖所有 I&T 相关成本、投资和折旧的管理和会计方法。使用企业的财务衡量系统进行报告。	a. 预期预算类别与实际预算类别之间的偏差的数量 b. 财务信息作为 I&T 资产和服务新投资业务案例的输入的实用性

活动	能力级别
1. 根据企业预算和成本会计政策和方法，确定 I&T 财务管理和会计的流程、输入、输出和责任。定义如何分析和报告（即向谁报告和如何报告）I&T 预算控制流程。	2
2. 定义分类方案，识别所有 I&T 相关成本要素（资本支出 [capex] 与运营支出 [opex]、硬件、软件、人员等）。确定如何获取这些要素。	
3. 使用财务信息为 I&T 资产和服务新投资业务案例提供输入。	3
4. 确保 I&T 资产和服务组合的成本得到维护。	
5. 建立并维护财务规划和经常性运营成本优化实践，以最少的支出为企业创造最大的价值。	4

相关指南（标准、框架、合规性要求）	详细参考
ITIL 第 3 版，2011 年	Service Strategy，4.3 Financial management for IT services

管理实践	指标示例
APO06.02 确定资源分配的优先顺序。 实施决策流程，确定资源分配的优先级，并建立针对各个业务部门的自主投资规定。包括考虑是否可能采用外部服务提供商，或者采用购买、开发、租赁的方式。	a. 已上报的资源分配问题的数量 b. I&T 资源与高优先级举措保持一致的百分比

活动	能力级别
1. 根据业务案例以及战略和战术优先级对所有 I&T 计划和预算请求进行排序。建立程序，确定预算分配和削减。	2
2. 在针对 I&T 促成的计划、服务和资产的高层次预算分配中分配业务和 IT 资源（包括外部服务提供商）。考虑购买或开发资本化的资产和服务，还是以按需付费的方式使用外部资产和服务。	
3. 建立沟通预算决策的程序，并与业务部门预算负责人一起审查。	
4. 识别、沟通和解决预算决策对业务案例、投资组合和战略计划的重大影响。例如，这可能包括由于企业环境变化而需要修改预算，或预算不足以支持战略目标或业务案例目标。	
5. 获得执行委员会对 I&T 预算影响（对实体的战略或战术计划产生负面影响）的批准。提出解决这些影响的行动建议。	3

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO06.03 编制和维护预算。 基于 I&T 促成的计划和 I&T 服务的组合，编制反映了投资重点的预算。	a. 疏忽和错误造成的预算变更的次数 b. I&T 预算在确定 I&T 促成的计划、服务和资产的所有预期 I&T 成本方面的实用性

A. 组件：流程（续）	
活动	**能力级别**
1. 实施正式的 I&T 预算，包括 I&T 促成的计划、服务和资产的所有预期 I&T 成本。	2
2. 在制定预算时，应考虑以下组件：与业务保持一致；与采购战略保持一致；获得授权的资金来源；内部资源成本，包括人员、信息资产和场所；第三方成本，包括外包合同、顾问和服务提供商；资本和运营支出；以及取决于工作量的成本要素。	
3. 记录证明意外情况合理性的理由，并定期审查。	
4. 为流程、服务和计划所有者以及项目和资产经理提供预算计划方面的指导。	
5. 审查预算计划并作出预算分配决策。根据不断变化的企业需求和财务因素编制和调整预算。	3
6. 考虑 I&T 促成的投资组合中记录的 I&T 项目以及资产和服务组合的运营和维护，记录、维护和沟通当前的 I&T 预算（包括承诺的支出和当前支出）。	
7. 监控不同预算方面的有效性。	4
8. 使用监控结果来实施改进并确保未来的预算更准确、可靠且更具成本效益。	5

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 20000-1:2011(E)	6.4 Budgeting and accounting for services
PMBOK Guide，第 6 版，2017 年	Part 1: 7. Project cost management

管理实践	指标示例
APO06.04 建立模型和分配成本。 创建并使用 I&T 成本计算模型，例如基于服务定义的 I&T 成本计算模型。这种方式可确保服务成本的分配是可识别、可衡量和可预测的，并鼓励组织负责地使用资源，包括服务提供商提供的资源。定期审查成本/分摊模型并进行基准检测，以维护模型与不断演变的业务和 IT 活动的相关性和适当性。	a. 根据商定的成本模型分配的总体 I&T 成本的百分比 b. 针对成本/分摊模型及其对不断变化的业务和 I&T 活动的适用性进行的审查和基准检测的次数

活动	能力级别
1. 确定成本分配模型，以推动面向用户的公平、透明、可重复和可比较的 I&T 相关成本分配。均摊共享 I&T 相关的成本便是一个基本的分配模型示例。这是一个非常简单、易于应用的分配模型，但根据企业环境，它往往被认为不公平且不利于鼓励组织负责地使用资源。基于活动的成本计算方案将成本分配到 IT 服务并向这些服务的用户收取费用，因而能够实现更透明和可比较的成本分配。	3
2. 检查服务定义目录，确定归入用户分摊类型的服务和归入共享服务类型的服务。	
3. 采用对用户有意义的类别和成本驱动因素（例如，每次客户服务部门呼叫的成本、每个软件许可的成本）设计足够透明的成本模型，使用户能够确定实际使用情况和费用，实现更好的 I&T 成本可预测性，以及更高效和有效地使用 I&T 资源。分析成本驱动因素（每项活动所花费的时间、费用、固定成本与可变成本的比例等）。确定适当的差异化（例如，不同类别的用户具有不同的权重），并且当实际成本存在很大变数时使用近似成本或平均值。	
4. 向关键利益相关方说明成本模型的原则和成果。获得他们的反馈并做出进一步调整，以实现透明和全面的模型。	
5. 获得关键利益相关方的批准，并与用户部门的管理层沟通 I&T 成本计算模型。	
6. 与关键利益相关方和用户部门的管理层沟通成本/分摊模型原则的重大变更。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
APO06.05 管理成本。 执行成本管理流程，比较预算成本和实际成本。组织应监控和报告成本。此外应及时识别偏差并评估其对企业流程和服务的影响。	a. 预算、预测与实际成本之间的偏差的百分比 b. 监控和报告偏差并评估其对企业流程和服务的影响的及时性

活动	能力级别
1. 获得关键利益相关方的批准，并与用户部门的管理层沟通 I&T 成本计算模型。	2
2. 根据预算和会计要求及时间表，确定成本管理流程的运作时间范围。	
3. 确定收集相关数据的方法，以确定预算与实际成本的偏差、投资 ROI、服务成本趋势等。	
4. 确定如何合并企业中适当层级的成本（中央 IT 预算与业务部门的 IT 预算）以及如何向利益相关方展示这些成本。报告中应提供每个成本类别的成本、预算与实际支出的比较状态、最高支出等相关信息，以及时识别需要的纠正措施。	3
5. 指导负责成本管理的人员捕获、收集和合并数据，并向相应的预算所有者展示和报告数据。预算分析师和所有者共同分析偏差并将绩效与内部和行业基准进行比较。他们应建立并维护日常开销的分摊方法。分析结果应提供重大偏差的说明和建议的纠正措施。	
6. 确保由适当层级的管理人员审查分析结果并批准建议的纠正措施。	
7. 确保识别成本结构和企业需求的变化，必要时修改预算和预测。	4
8. 定期寻找在不危及服务的前提下优化成本和提高效率的方法，尤其是在财务限制造成预算削减的情况下。	5

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构						
关键管理实践	**首席财务官**	**首席信息官**	**首席技术官**	**首席数字官**	**组合经理**	**IT 行政总监**
APO06.01 管理财务和会计。	A				R	R
APO06.02 确定资源分配的优先顺序。	R	A	R	R	R	R
APO06.03 编制和维护预算。	R	A	R	R		R
APO06.04 建立模型和分配成本。	R	A				R
APO06.05 管理成本。	R	A	R	R		R

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：管理流程和项目（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
APO06.01 管理财务和会计。	BAI09.01	资产登记表	财务规划实践	内部
			I&T 成本分类方案	内部
			会计流程	内部
APO06.02 确定资源分配的优先顺序。	APO04.04	概念验证范围和业务案例大纲	预算分配	APO02.05；APO05.02；APO07.05；BAI03.11
	APO05.01	投资回报预期	确定 I&T 举措的优先级和评级	APO05.02
	APO05.02	• 计划业务案例 • 业务案例评估		
	EDM02.02	投资和服务组合的评估		
	EDM02.04	改进实现价值的措施		
APO06.03 编制和维护预算。			I&T 预算	APO02.05；APO05.02；APO07.01；BAI03.11
			预算沟通	APO05.02；APO07.01；BAI03.11
APO06.04 建立模型和分配成本。			运营程序	内部
			成本分配沟通	内部
			成本分配模型	内部
			已分类的 I&T 成本	内部
APO06.05 管理成本。	BAI01.02	计划的效益实现规划	成本优化机会	APO02.02
	BAI01.04	计划预算和效益登记表	成本整合方法	内部
	BAI01.05	效益实现的监控结果	成本数据收集方法	内部
	EDM02.04	组合和计划绩效的反馈		

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 7. Project cost management: Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
财务管理	Skills Framework for the Information Age，第 6 版，2015 年	FMIT

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
预算政策	阐明年度预算的准备和时间表以及年度财务状况的预测。概述所需的管理报告流程。确定预算计划和其他财务文件的职责和责任。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
要高效和有效地管理 I&T，应在整个组织内形成提供透明的预算、成本和效益的文化。管理层应促成基于事实的决策文化，例如通过业务和 IT 可比较的成本与效益估算，为组合管理、IT 资产和资源的成本公平分配，以及可重复的 IT 预算提供输入。		

G. 组件：服务、基础设施和应用程序
成本会计系统

领域：调整、规划和组织 管理目标：APO07 — 妥当管理的人力资源	焦点领域：COBIT 核心模型

描述

提供结构化方法以确保最佳的人力资源（内部和外部）招聘/获取、规划、评估和开发。

目的

优化人力资源能力，以实现企业目标。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG10 员工技能、动力和生产力 • EG13 产品和业务创新	• AG12 既了解技术又熟知业务、能力出众且积极上进的员工 • AG13 业务创新的知识、专业技能和举措

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG12	a. 精通 I&T 的业务人员（即具备必要的 I&T 知识且了解 I&T，能够引导、指导、创立和发现在其业务专业领域运用 I&T 的机会）的百分比 b. 精通业务的 I&T 人员（即具备必要的相关业务领域知识和理解，能够引导、指导、创立和发现在业务领域运用 I&T 的机会）的百分比 c. 拥有技术管理经验的业务人员的数量或百分比
EG10	a. 相较于基准的员工生产力 b. 利益相关方对员工专业知识和技能的满意度 c. 相对其角色所需能力而言技能不足的员工的百分比 d. 满意员工的百分比	AG13	a. 业务高管对 I&T 创新可能性的认识和理解水平 b. 源自 I&T 创新想法的已批准举措的数量 c. 获得认可/奖励的创新推动者的数量
EG13	a. 对业务创新机会的认识和理解水平 b. 利益相关方对产品以及创新专长和想法的满意度 c. 源自创新想法的已批准产品和服务举措的数量		

A. 组件：流程

管理实践	指标示例
APO07.01 获取和维护足够且适当的人员配备。 建立并维护涵盖所有 I&T 相关成本、投资和折旧的管理和会计方法，作为企业财务系统和会计科目表不可或缺的一部分。使用企业的财务衡量系统进行报告。	a. 职位空缺的平均持续时间 b. IT 职位空缺的百分比 c. 员工流失率

活动	能力级别
1. 定期或在发生重大变更时评估人员配备要求。确保企业和 IT 职能部门都有充足的资源来充分合理地支持企业目的和目标、业务流程和控制以及 I&T 促成的举措。	2
2. 根据整个企业的人事政策和程序维护业务和 IT 人员的招聘和保留流程。	
3. 灵活地安排资源（例如采用转岗、外部承包商和第三方服务安排），以支持不断变化的业务需求。	
4. 将背景调查纳入 IT 部门的员工、承包商和供应商招募流程中。调查的范围和频率应取决于职能的敏感度和/或关键性。	3

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
COSO Enterprise Risk Management，2017 年 6 月	6. Governance and Culture—Principle 5
Skills Framework for the Information Age，第 6 版，2015 年	SFIA and skills management—Acquire
管理实践	**指标示例**
APO07.02 识别关键 IT 人员。 识别关键 IT 人员。利用知识获取（记录）、知识共享、接班计划和配备后备人员，最大限度减少因唯一人员承担关键工作职能而导致的对唯一人员的依赖性。	a. 企业依赖唯一人员承担的关键工作的百分比 b. 已执行的后备人员配备计划的数量

活动	能力级别
1. 作为一项安全预防措施，提供关键人员最短年度休假时间方面的准则。	2
2. 采取适当的工作变更措施（尤其是工作终止）。	
3. 通过知识获取（记录）、知识共享、接班计划、配备后备人员、交叉培训以及岗位轮换举措，最大限度减少因唯一人员承担关键工作职能而导致的对唯一人员的依赖性。	
4. 定期测试后备人员配备计划。	3

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	RI.RR Identification of Roles and Responsibilities
Skills Framework for the Information Age，第 6 版，2015 年	SFIA and skills management—Acquire
管理实践	**指标示例**
APO07.03 保持人员的技能和能力。 定义和管理人员所需的技能和能力。根据相关人员的教育、培训和/或经验，定期检查其是否有能力履行其职责。在适当的情况下，通过资质验证和认证计划确认这些能力是否得到保持。为员工提供持续学习并保持技能、知识和能力的机会，使员工能力保持在能够实现企业目标的水平上。	a. 资源矩阵中确定缺乏的关键技能和能力 b. 所需技能与可用技能之间已确定的差距数量 c. 已提供的培训计划的数量

活动	能力级别
1. 确定内部和外部资源当前可用的技能和能力。	2
2. 确定所需技能与可用技能之间的差距。制定行动计划，例如培训（技术和行为技能）、招聘、重新部署和人才挖掘战略的变更，以弥补个体和集体存在的差距。	
3. 定期审查培训材料和计划。确保它们充分体现不断变化的企业要求及其对所需的知识、技术和能力的影响。	3
4. 提供知识库的访问权限，以支持技能和能力发展。	
5. 根据组织和流程要求制定并实施培训计划，包括对企业知识、内部控制、道德行为以及安全和隐私的要求。	
6. 开展定期审查，评估内部和外部资源的技能和能力的发展情况。审查接班计划。	4

相关指南（标准、框架、合规性要求）	详细参考
ISF, The Standard of Good Practice for Information Security 2016	PM2.3 Security Education/Training
ISO/IEC 27001:2013/Cor.2:2015(E)	7.2 Competence
美国国家标准与技术研究所，Framework for Improving Critical Infrastructure Cybersecurity，第 1.1 版，2018 年 4 月	PR.AT Awareness and Training
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.2 Awareness and training (AT-3, AT-4)
Skills Framework for the Information Age，第 6 版，2015 年	SFIA and skills management—Deploy
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

A. 组件：流程（续）	
管理实践	**指标示例**
APO07.04 评估和认可/奖励员工工作绩效。 定期对照从企业目标、既定标准、特定工作职责以及技能和能力框架派生的个人目标，及时开展绩效评估。实施薪酬/认可流程，以奖励成功达成绩效目标的人员。	a. 已执行的正式反馈和 360 度评估的次数 b. 给予员工奖励的次数和价值

活动	能力级别
1. 基于职能部门/企业目标来设定个人目标。	2
2. 设定与相关 I&T 和企业目标一致的个人目标。基于明确性、可衡量性、可实现性、相关性和时限性 (SMART) 原则设定目标，以反映角色所需的核心能力、企业价值和技能。	
3. 对照个人目标提供及时的绩效反馈。	
4. 提供关于在评估过程中使用和存储个人信息的具体说明，以遵从适用的个人数据和就业法规。	
5. 整理 360 度绩效评估的结果。	3
6. 根据评估流程的结果，提供正式的职业规划和职业发展计划，以鼓励员工发展能力，提供个人发展机会，以及减少对关键人员的依赖。在适当的情况下为员工提供绩效和行为指导。	
7. 实施薪酬/认可流程，以奖励履行承诺、发展能力和成功达成绩效目标的人员。确保流程实施一致且符合组织政策。	
8. 实施和沟通纪律处分流程。	

相关指南（标准、框架、合规性要求）	详细参考
Skills Framework for the Information Age，第 6 版，2015 年	SFIA and skills management—Develop

管理实践	指标示例
APO07.05 计划和跟踪 IT 和业务的人力资源使用情况。 了解并跟踪对负有企业 I&T 职责的业务和 IT 人力资源的当前和未来需求。确定短缺数量并对资源开发计划、企业和 IT 招聘流程以及业务和 IT 招聘流程提供意见。	a. 人员配备计划中已确定的资源短缺和技能缺失的数量 b. 每位等量全职员工 (FTE) 花在任务和项目上的时间

活动	能力级别
1. 创建并维护业务和 IT 人力资源清单。	2
2. 了解当前和未来的人力资源需求，以支持实现 I&T 目标，以及根据当前 I&T 相关举措的组合、未来的投资组合和日常运营需求提供服务和解决方案。	3
3. 确定短缺数量并对资源开发计划以及企业和 IT 招聘流程提供意见。制定和审查人员配备计划，并跟踪实际执行情况。	
4. 针对花在不同任务、指派、服务或项目上的时间维护足够的信息。	4

相关指南（标准、框架、合规性要求）	详细参考
Skills Framework for the Information Age，第 6 版，2015 年	SFIA and skills management—Assess; Reward

管理实践	指标示例
APO07.06 管理合同人员。 确保使用 I&T 技能为企业提供支持的咨询顾问及合同人员均了解并遵守组织政策且满足协定的合同要求。	a. 签字同意企业控制框架的承包商的百分比 b. 旨在确保承包商员工的正确性和合规性的定期审查的频率

A. 组件：流程（续）	
活动	**能力级别**
1. 实施合同人员政策和程序。	2
2. 在合同开始时获得承包商的正式同意，要求他们遵守企业的 I&T 控制框架，例如安全许可政策、物理和逻辑访问控制、设施使用、信息保密要求和保密协议。	
3. 告知承包商：管理层保留监控和检查所有 IT 资源使用情况的权利，包括电子邮件、语音通信以及所有程序和数据文件。	
4. 在合同中明确定义承包商的角色和职责，包括根据商定的标准和格式记录其工作的明确要求。	
5. 审查承包商的工作并根据结果批准付款。	
6. 通过正式和明确的合同定义由外部各方执行的所有工作。	3
7. 定期开展审查，以确保合同人员已签署并同意所有必要的协议。	4
8. 定期开展审查，以确保承包商的角色和访问权限适当且符合协议。	

相关指南（标准、框架、合规性要求）	详细参考
Skills Framework for the Information Age，第 6 版，2015 年	SFIA and skills management—Deploy

B. 组件：组织结构																	
关键管理实践	**首席财务官**	**首席运营官**	**首席信息官**	**首席技术官**	**首席数字官**	**项目管理办公室**	**人力资源总监**	**架构总监**	**开发总监**	**IT 运营总监**	**IT 行政总监**	**服务经理**	**信息安全经理**	**业务连续性经理**	**隐私官**	**法律顾问**
APO07.01 获取和维护足够且适当的人员配备。			A	R	R	R	R	R	R	R	R	R	R	R		
APO07.02 识别关键 IT 人员。			A	R	R	R	R	R	R	R	R	R	R	R	R	R
APO07.03 保持人员的技能和能力。			A	R	R	R	R	R	R	R	R	R	R	R		
APO07.04 评估和认可/奖励员工工作绩效。			A			R	R	R	R	R	R	R	R	R		
APO07.05 计划和跟踪 IT 和业务的人力资源使用情况。	R	A	R	R	R	R	R	R	R	R	R	R	R	R		
APO07.06 管理合同人员。			A	R	R	R	R	R	R	R	R	R	R	R		R

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	**输入**		**输出**	
APO07.01 获取和维护足够且适当的人员配备。	**自**	**描述**	**描述**	**至**
	APO01.05	监督实践的定义	工作说明和人员挖掘计划	内部
	APO06.03	• IT 预算 • 预算沟通	人员配置要求评估	内部
	EDM04.01	• 资源和能力分配的指导原则 • 已批准的资源计划	能力和职业发展计划	内部；APO07.02
	EDM04.03	解决资源管理偏离的补救措施		
	在 COBIT 外部	• 企业人力资源政策与程序 • 企业目的和目标		
APO07.02 识别关键 IT 人员。	APO07.01	能力和职业发展计划	工作终止行动计划	内部
			关于最短假期的指导	内部
APO07.03 保持人员的技能和能力。	APO01.08	目标技能和能力矩阵	技能和能力矩阵	APO01.05；APO14.01 BAI01.02；BAI01.04；BAI03.12
	BAI08.02	已发布的知识贮存库	技能培养计划	APO01.05；EDM04.01
	BAI08.03	知识意识和培训方案	审查报告	内部
	DSS04.06	• 培训要求 • 技能和能力的监控结果		
	EDM01.02	激励系统方法		
	EDM04.03	解决资源管理偏离的补救措施		
	在 COBIT 外部	企业目的和目标		

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
APO07.04 评估和认可/奖励员工工作绩效。	**自**	**描述**	**描述**	**至**
	APO04.01	认可与奖励计划	改进计划	内部
	BAI05.04	调整的 HR 绩效目标	绩效评估	内部
	BAI05.06	HR 绩效审查结果	人员目标	内部
	DSS06.03	分配的访问权限		
	EDM01.02	激励系统方法		
	在 COBIT 外部	企业目的和目标		
APO07.05 计划和跟踪 IT 和业务的人力资源使用情况。	APO06.02	预算分配	业务和 IT 人力资源清单	BAI01.04
	BAI01.04	资源要求和角色	资源使用记录	BAI01.06
	BAI11.08	项目资源要求	资源短缺分析	BAI01.06
	EDM04.02	资源配置战略的沟通		
	EDM04.03	对资源和能力分配及有效性的反馈		
	企业组织	当前和未来组合		
	在 COBIT 外部	企业组织结构		
APO07.06 管理合同人员。	BAI01.04	资源要求和角色	合同协议审查	内部
	BAI01.09	计划终止和持续责任的沟通	合同协议	内部
	BAI11.08	项目资源要求	合同人员政策	内部
相关指南（标准、框架、合规性要求）		**详细参考**		
PMBOK Guide，第 6 版，2017 年		Part 1: 9. Project resource management: Inputs and Outputs		

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
教育和培训的提供	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	D. Enable—D.3. Education and Training Provision
学习和发展管理	Skills Framework for the Information Age，第 6 版，2015 年	ETMG
绩效管理	Skills Framework for the Information Age，第 6 版，2015 年	PEMT
个人发展	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework，2016 年	D. Enable—D.9. Personnel Development
职业发展	Skills Framework for the Information Age，第 6 版，2015 年	PDSV
资源配置	Skills Framework for the Information Age，第 6 版，2015 年	RESC

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
合同人员政策	列举根据企业 IT 采购政策和 I&T 控制框架增加第三方顾问和/或承包商人员的标准。规定在何种条件下、何时可以由第三方执行或增加哪些工作类型。	美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.16 Personnel security (PS-1)
人力资源 (HR) 政策	概述企业及其员工的共同期望。列举行为准则中可接受和不可接受的员工行为，以帮助管理与人为行为有关的风险。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
描述用户在信息、媒体和网络使用以及安全和隐私方面的角色和责任。鼓励和传播一种规定了企业中所有人员的预期行为以及对不道德行为的零容忍的共同文化。	美国国家标准与技术研究所特别出版物 800-53，修订版 5，2017 年 8 月	3.14 Planning (PL-4)

G. 组件：服务、基础设施和应用程序
• HR 管理系统 • 绩效衡量系统（例如平衡计分卡、技能管理工具） • 资源计划工具

领域：调整、规划和组织 管理目标：APO08 — 妥当管理的关系	焦点领域：COBIT 核心模型

描述

以正式和透明的方式管理与业务利益相关方的关系，确保相互信任，并共同致力于在预算和风险容忍度限制内实现战略目标。将关系建立在公开和透明的沟通、共同语言以及双方都愿意为关键决策承担所有权和责任的基础之上。业务和 IT 必须协同工作，以取得成功的企业成果来支持企业目标。

目的

掌握正确的知识、技能和行为，来创造更好的成果，增强信心和相互信任，以及有效地利用资源，以促进与业务利益相关方建立富有成效的关系。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化 • EG10 员工技能、动力和生产力 • EG13 产品和业务创新	• AG05 提供符合业务需求的 I&T 服务 • AG06 将业务需求转化为可运作的解决方案的敏捷性 • AG12 既了解技术又熟知业务、能力出众且积极上进的员工 • AG13 业务创新的知识、专业技能和举措

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG05	a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度	AG06	a. 业务高管对 I&T 响应新需求的满意度水平 b. 新的 I&T 相关服务和应用程序的平均上市时间 c. 将战略 I&T 目标转化为议定的已批准举措所需的平均时间 d. 受最新基础设施和应用支持的关键业务流程的数量
EG10	a. 相较于基准的员工生产力 b. 利益相关方对员工专业知识和技能的满意度 c. 相对其角色所需能力而言技能不足的员工的百分比 d. 满意员工的百分比	AG12	a. 精通 I&T 的业务人员（即具备必要的 I&T 知识且了解 I&T，能够引导、指导、创立和发现在其业务专业领域运用 I&T 的机会）的百分比 b. 精通业务的 I&T 人员（即具备必要的相关业务领域知识和理解，能够引导、指导、创立和发现在业务领域运用 I&T 的机会）的百分比 c. 拥有技术管理经验的业务人员的数量或百分比
EG13	a. 对业务创新机会的认识和理解水平 b. 利益相关方对产品以及创新专长和想法的满意度 c. 源自创新想法的已批准产品和服务举措的数量	AG13	a. 业务高管对 I&T 创新可能性的认识和理解水平 b. 源自 I&T 创新想法的已批准举措的数量 c. 获得认可/奖励的创新推动者的数量

A. 组件：流程	
管理实践	**指标示例**
APO08.01 了解业务期望。 了解当前的业务问题和目标以及对 I&T 的期望。确保要求得到理解、管理和沟通，并且其状态通过议定和审批。	a. 已识别的当前业务问题的数量 b. 为 I&T 促成的服务定义的业务要求的数量

活动	能力级别
1. 确定业务利益相关方及其利益和职责范围。	2
2. 审查当前的企业方向、问题、战略目标以及与企业架构的一致性。	
3. 了解当前的业务环境、流程限制或问题、地理扩张或收缩以及行业/监管驱动因素。	
4. 维护对业务流程和相关活动的认识。了解与服务量和使用相关的需求模式。	
5. 通过确保业务部门了解请求的优先级、依存关系、财务限制以及安排请求的需求来管理期望。	3
6. 阐明对 I&T 促成的服务和解决方案的业务期望。确保使用相关的业务验收标准和指标来定义需求。	4
7. 确保 IT 与所有业务部门就期望及其衡量方式达成协议。确保所有利益相关方确认此协议。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO08.02 使 I&T 战略与业务期望保持一致，并识别通过 IT 增强业务的机会。 使 I&T 战略与当前的业务目标和期望保持一致，从而让 IT 成为业务部门的增值合作伙伴和增强企业绩效的治理组件。	a. 技术机会在投资方案中的纳入率 b. 关于业务利益相关方的技术意识水平的调查

活动	能力级别
1. 将 IT 视为业务部门的合作伙伴。积极地确定机会、风险和限制并与关键利益相关方进行沟通。这包括当前和新兴的技术、服务和业务流程模型。	3
2. 通过组合、计划和项目管理，就重大新举措开展合作。确保 IT 组织从一开始就参与到新举措中，提供能够增加价值的建议（例如针对业务案例开发、需求定义、解决方案设计的建议）并获取 I&T 工作流的所有权。	

相关指南（标准、框架、合规性要求）	详细参考
ITIL 第 3 版，2011 年	Service Strategy，4.4 Demand management

管理实践	指标示例
APO08.03 管理业务关系。 管理 IT 服务组织与其业务合作伙伴的关系。确保定义和分配在维护关系方面的角色和职责，并促进沟通。	a. 用户与 IT 人员满意度调查的评级 b. 已定义、分配和沟通的关系角色和职责的百分比

活动	能力级别
1. 任命一名关系经理作为各个重要业务部门的单一联络点。确保在业务组织中确定一位对应人员，这位员工不仅要了解业务，还应具备足够的技术意识和适当的权限级别。	3
2. 以正式、透明的方法管理关系，确保专注于实现一个共同目标，即在预算和风险容忍度限制内取得支持战略目标的成功企业成果。	
3. 定义并沟通用于解决任何关系问题的投诉和上报程序。	
4. 确保关键决策得到相关的责任利益相关方的同意和批准。	
5. 根据共同商定的目标和共同语言（服务和绩效审查会议、新战略或计划的审查等）计划详细的互动和时间表。	4

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
ISO/IEC 20000-1:2011(E)	7.1 Business relationship management
ITIL 第 3 版，2011 年	Service Strategy，4.5 Business relationship management
管理实践	**指标示例**
APO08.04 协调和沟通。 与所有利益相关方合作，协调如何以端到端的方式为业务提供 I&T 服务和解决方案。	a. 距离上次更新与业务部门的端到端沟通计划的时间 b. 业务所有者对 I&T 服务和解决方案的端到端交付方面的协调工作感到满意的百分比

活动	能力级别
1. 协调和沟通变更和过渡活动，例如项目或变更计划、时间表、发布政策、发布已知错误和培训意识。	2
2. 协调和沟通运营活动、角色和职责，包括请求类型的定义、分级上报、重大中断（计划内和计划外），以及服务报告的内容和频率。	
3. 承担响应可能影响与业务部门关系的重大事件的责任。必要时提供直接支持。	
4. 维护端到端沟通计划，其中定义了服务交付信息的内容、频率和接收者，包括已交付价值和任何已识别风险的状态。	3

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO08.05 对持续改进服务提供意见。 持续改进和发展 I&T 促成的服务和企业服务交付，以应对不断变化的企业目标和技术	a. I&T 服务与企业业务要求保持一致的百分比 b. 已确定并解决任何问题的根本原因的百分比

活动	能力级别
1. 执行客户和提供商满意度分析。确保问题得到解决并报告结果和状态。	4
2. 共同确定、沟通和实施改进举措。	5
3. 与服务管理和流程所有者合作，确保不断改进 I&T 促成的服务和服务管理流程，以及确定和解决任何问题的根本原因。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构																	
关键管理实践	首席执行官	首席财务官	首席运营官	首席信息官	首席技术官	首席数字官	I&T 治理委员会	业务流程所有者	关系经理	架构总监	开发总监	IT 运营总监	服务经理	信息安全经理	业务连续性经理	隐私官
APO08.01 了解业务期望。				A	R	R		R	R		R	R	R	R	R	R
APO08.02 使 I&T 战略与业务期望保持一致，并识别通过 IT 增强业务的机会。				A	R	R	R	R	R	R	R	R	R			
APO08.03 管理业务关系。	R	R	R	A	R	R		R	R		R	R	R			
APO08.04 协调和沟通。	R	R	R	A	R	R		R	R		R	R	R			
APO08.05 对持续改进服务提供意见。				A	R	R		R	R		R	R	R			

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
APO08.01 了解业务期望。	APO02.05	战略路线图	已阐明和商定的业务期望	内部
APO08.02 使 I&T 战略与业务期望保持一致，并识别通过 IT 增强业务的机会。	APO09.01	已确定的为业务提供的 IT 服务的差距	已商定的后续步骤和行动计划	内部
	APO09.04	• 服务水平绩效报告 • 改进行动计划和补救措施		
	APO11.03	未能提供高品质的根本原因		
APO08.03 管理业务关系。	DSS02.02	已分类并排定优先级的事故和服务请求	投诉和上报状态	内部
	DSS02.06	• 已关闭的服务请求和事故 • 用户确认对服务的履行或问题的解决感到满意	商定的关键决策	内部
	DSS02.07	• 事故状态和趋势报告 • 请求履行状态和趋势报告		

C. 组件：信息流和信息项（另请参阅第 3.6 节）（续）				
管理实践	输入		输出	
APO08.04 协调和沟通。	自	描述	描述	至
	APO09.03	服务水平协议 (SLA)	客户响应	内部
	APO12.06	风险影响的沟通	沟通工作包	内部
	BAI05.05	操作和使用计划	沟通计划	内部
	BAI07.07	补充性支持计划		
	BAI09.02	关于计划内维护停机时间的沟通		
	DSS03.04	所学知识的沟通		
APO08.05 对持续改进服务提供意见。	APO09.02	服务目录	潜在改进项目的定义	APO02.02；BAI03.11
	APO11.02	• 客户对质量管理的要求 • 服务质量的结果，包括客户反馈	满意度分析	APO09.04
	APO11.03	对解决方案和服务交付的质量监控结果		
	APO11.04	质量审查和审计的结果		
	BAI03.10	维护计划		
	BAI05.05	成功衡量指标和结果		
	BAI07.07	补充性支持计划		
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
关系管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage—E.4. Relationship Management
关系管理	Skills Framework for the Information Age，第 6 版，2015 年	RLMT

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
业务 - IT 关系管理政策	提供关于建立和维护业务与 IT 之间关系的准则。促进透明度和相互信任，并共同致力于在预算和风险容忍度范围内实现战略目标。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
建立基于相互信任、透明沟通、开放和可理解的术语及共同语言、所有权和问责制的文化。企业内必须建立良好的业务与 IT 关系才能实现共同目标。		

G. 组件：服务、基础设施和应用程序
• 协作平台 • 内部培训和意识培养服务

领域：调整、规划和组织 管理目标：APO09 — 妥当管理的服务协议	焦点领域：COBIT 核心模型

描述

使 I&T 促成的产品和服务及服务水平与企业需求和期望保持一致，包括识别、规范、设计、发布、协商以及对 I&T 产品和服务、服务水平及绩效指标的监控。

目的

确保 I&T 产品、服务和服务水平满足当前和未来的企业需求。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化	AG05 提供符合业务需求的 I&T 服务
企业目标的指标示例	**一致性目标的指标示例**
EG01 a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG05 a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG08 a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度	

A. 组件：流程

管理实践	指标示例
APO09.01 识别 I&T 服务。 分析业务要求以及I&T 促成的服务和服务水平支持业务流程的程度。与业务部门讨论和商定潜在的服务和服务水平。将潜在的服务水平与当前的服务组合进行比较；识别新的或变更的服务或服务水平选项。	a. 未得到任何 I&T 服务支持的业务活动的数量 b. 识别的过时服务的数量

活动	能力级别
1. 评估当前的 I&T 服务和服务水平，以识别现有服务与其支持的业务活动之间的差距。识别现有服务和服务水平选项需要改进的方面。	2
2. 分析、研究和评估未来的需求，并确认 I&T 促成的现有服务的能力。	
3. 分析业务流程活动，识别对新的或重新设计的 I&T 服务的需求。	3
4. 将已识别的需求与组合中现有的服务组件进行比较。如果可能，将现有的服务组件（I&T 服务、服务水平选项和服务包）打包为新的服务包，以满足所识别的业务需求。	
5. 定期与组合管理人员和业务关系管理人员审查 I&T 服务组合，以识别过时的服务。商定服务停用并提出变更建议。	
6. 在可能的情况下，将需求与服务包进行匹配，并创建标准化服务以实现总体效率。	4

相关指南（标准、框架、合规性要求）	详细参考
ITIL 第 3 版，2011 年	Service Strategy, 4.4 Demand management

A. 组件：流程（续）	
管理实践	**指标示例**
APO09.02 将 I&T 促成的服务编成目录。 为相关目标团队定义和维护一份或多份服务目录。在服务目录中发布和维护在用 I&T 促成的服务。	a. 提供的在用 I&T 促成的服务和服务包相对于组合的百分比 b. 自上次更新服务组合以来的时间
活动	**能力级别**
1. 在目录中发布相关的在用 I&T 促成的服务、服务包和组合中的服务水平选项。	2
2. 持续确保组合中的服务组件和相关的服务目录是完整且最新的。	3
3. 将服务目录的任何更新通知业务关系管理人员。	
相关指南（标准、框架、合规性要求）	**详细参考**
ITIL 第 3 版，2011 年	Service Design, 4.2 Service Catalogue Management
管理实践	**指标示例**
APO09.03 确定和拟定服务协议。 根据服务目录中的选项定义和准备服务协议。包括内部运营协议。	a. 未确定服务协议的业务流程数量 b. 有服务协议涵盖的在用 IT 服务的百分比
活动	**能力级别**
1. 分析从业务关系管理人员收到的新增或变更服务协议的需求，确保能够匹配这些需求。考虑以下方面：服务时间、可获取性、性能、能力、安全性、隐私性、连续性、合规性以及监管问题、可用性、需求限制和数据质量。	2
2. 基于相关服务目录中的服务、服务包和服务水平选项，草拟客户服务协议。	
3. 与业务关系管理人员最终确定客户服务协议。	
4. 确定、商定并记录内部运营协议，以支持客户服务协议（如适用）。	3
5. 与供应商管理人员保持联系，确保与外部服务提供商签订适当的商业合同来支持客户服务协议（如适用）。	
相关指南（标准、框架、合规性要求）	**详细参考**
ISF, The Standard of Good Practice for Information Security 2016	SY2.1 Service Level Agreements
ISO/IEC 20000-1:2011(E)	4.5 Establish and improve the SMS; 6.1 Service level management
ITIL 第 3 版，2011 年	Service Design, 4.3 Service Level Management
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.18 System and services acquisition (SA-9)
管理实践	**指标示例**
APO09.04 监控和报告服务水平。 监控服务水平、报告实现情况和识别趋势。提供适当的管理信息以辅助绩效管理。	a. 服务违规的数量和严重程度 b. 认为服务交付满足议定水平的客户的百分比 c. 满足服务目标的百分比 d. 按照服务水平进行监控的服务的百分比
活动	**能力级别**
1. 制定和维护用于监控和收集服务水平数据的措施。	4
2. 评估绩效，并定期提供服务协议绩效的正式报告，包括偏离议定值的情况。将该报告分发给业务关系管理人员。	
3. 定期进行审查，以预测和识别服务水平绩效的趋势。将质量管理实践纳入服务监控中。	
4. 提供适当的管理信息以辅助绩效管理。	
5. 商定针对任何绩效问题或负面趋势的行动计划和补救措施。	
相关指南（标准、框架、合规性要求）	**详细参考**
HITRUST CSF，第 9 版，2017 年 9 月	09.02 Control Third Party Service Delivery
ISO/IEC 20000-1:2011(E)	6.2 Service reporting

A. 组件：流程（续）	
管理实践	**指标示例**
APO09.05 审查服务协议和合同。 定期审查服务协议并根据需要进行修改。	a. 执行的服务协议审查次数 b. 满足服务目标的百分比 c. 对服务协议质量满意的利益相关方的百分比 d. 根据需要修订的服务协议的数量

活动	能力级别
1. 根据商定的条款定期审查服务协议，确保协议的有效性和保持更新。适当情况下，考虑需求、I&T 促成的服务、服务包或服务水平选项的变化。	3
2. 根据需要，与服务提供商一起修订现有的服务协议。商定并更新内部运营协议。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构												
关键管理实践	**首席运营官**	**首席信息官**	**首席技术官**	**企业风险委员会**	**业务流程所有者**	**IT 运营总监**	**IT 行政总监**	**服务经理**	**信息安全经理**	**隐私官**	**法律顾问**
APO09.01 识别 I&T 服务。	R	R	A		R			R			
APO09.02 将 I&T 促成的服务编成目录。		R	A	R				R			
APO09.03 确定和拟定服务协议。		R	A			R	R	R	R	R	R
APO09.04 监控和报告服务水平。		R	A		R			R			R
APO09.05 审查服务协议和合同。	R	A	R			R	R	R			

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 20000-1:2011(E)	4.1.1 Management commitment

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
APO09.01 识别 I&T 服务。	自	描述	描述	至
			已确定的为业务提供的 I&T 服务的差距	APO01.10；APO02.02；APO05.02；APO08.02
			标准服务的定义	EDM02.01
APO09.02 将 I&T 促成的服务编成目录。	APO05.04	更新的计划、服务和资产组合	服务目录	APO08.05
	EDM04.01	已批准的资源计划		
	EDM04.02	资源配置战略的沟通		
APO09.03 确定和拟定服务协议。	APO11.02	客户对质量管理的要求	服务水平协议 (SLA)	APO05.02；APO08.04；DSS01.02；DSS02.01；DSS02.02；DSS04.01；DSS05.02；DSS05.03
	APO14.07	数据质量要求	运营水平协议 (OLA)	DSS01.02；DSS02.07；DSS04.03；DSS05.03
APO09.04 监控和报告服务水平。	APO05.03	投资组合绩效报告	改进行动计划和补救措施	APO02.02；APO08.02
	APO05.05	• 效益结果和相关沟通 • 用于改进效益实现的纠正措施	服务水平绩效报告	APO08.02；MEA01.03
	APO08.05	满意度分析		
	APO11.03	• 对解决方案和服务交付的质量监控结果 • 交付质量失败的根本原因		
	APO11.04	质量审查和审计的结果		
	DSS02.02	已分类并排定优先级的事故和服务请求		
	DSS02.06	已关闭的服务请求和事故		
	DSS02.07	• 事故状态和趋势报告 • 请求履行状态和趋势报告		
	EDM04.03	解决资源管理偏离的补救措施		

C. 组件：信息流和信息项（另请参阅第 3.6 节）（续）				
管理实践	输入		输出	
APO09.05 审查服务协议和合同。	自	描述	描述	至
	APO11.02	服务质量的结果，包括客户反馈	更新的 SLA	内部
	APO11.04	质量审查和审计的结果		
	BAI04.01	参照 SLA 进行的评估		
	EDM04.03	对资源和能力分配及有效性的反馈		

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 12. Project procurement management: Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
服务水平管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	A. Plan—A.2. Service Level Management
服务水平管理	Skills Framework for the Information Age，第 6 版，2015 年	SLMO

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
服务水平协议 (SLA) 政策	描述通用标准和衡量准则，以说明关于服务交付的具体要求和条款（无论是企业内的实体之间还是企业与第三方之间）。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
在服务提供商（内部或外部）与最终用户之间订立合同，定义预期的服务水平。确保此服务水平以输出为基础，并以 SMART 目标（明确性、可衡量性、可实现性、真实性和时限性）的形式具体定义客户可获得的服务。建立尊重服务水平的文化。通过惩罚体制遏制不合规行为。		

G. 组件：服务、基础设施和应用程序
• 合同管理系统 • 服务水平监控工具

领域：调整、规划和组织 管理目标：APO10 — 妥当管理的供应商	焦点领域：COBIT 核心模型

描述

管理各类供应商提供的 I&T 相关产品及服务以满足企业需求。这包括搜寻和选择供应商、关系管理、合同管理，以及审查与监控供应商绩效和供应商生态系统（包括上游供应链）的有效性和合规性。

目的

优化可用的 I&T 能力，以支持 I&T 战略和路线图，最大程度地降低与不履约或不合规供应商相关的风险，并确保有竞争力的定价。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化	AG05 提供符合业务需求的 I&T 服务

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG05	a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		

A. 组件：流程

管理实践	指标示例
APO10.01 确定和评估供应商关系与合同。 持续搜寻和确定供应商，并根据类型、重要性和关键性进行分类。制定供应商和合同的评估准则。审查现有和备选供应商与合同的总体组合。	a. 现有供应商和合同达到规定的评估准则的百分比 b. 提供与现有供应商合同中同等服务的备选供应商的百分比

活动	能力级别
1. 持续审视企业环境，搜寻可以提供互补能力和支持实现I&T 战略、路线图及企业目标的新合作伙伴和供应商。	3
2. 制定和维护与供应商及供应商合同的类型、重要性和关键性相关的衡量准则，以关注首选的和重要的供应商。	
3. 根据规定的衡量准则识别、记录和归类现有的供应商和合同，以维护需要认真管理的首选供应商详细登记表。	
4. 制定和维护供应商及合同评估准则，以一致的方式全面审查和比较供应商绩效。	4
5. 定期评估和比较现有供应商与备选供应商的绩效，以发现机会重新考虑目前供应商合同或迫切需要。	5

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
APO10.02 选择供应商。 按照公平和正式的做法选择供应商，基于指定需求，确保选出最契合组织的供应商。应根据潜在供应商的意见优化需求。	a. 所选供应商的产品服务与需求建议书 (RFP) 中所指定需求之间已识别的差距个数 b. 对供应商满意的利益相关方的百分比

活动	能力级别
1. 审查所有信息请求 (RFI) 和需求建议书 (RFP)，确保它们明确定义了相关要求（例如，企业对于信息安全及隐私的要求、运营业务和 I&T 处理要求、服务交付的优先级等），并包含澄清要求的程序。RFI 和 RFP 应允许供应商有充足的时间准备他们的建议，并应明确规定奖励准则和决策流程。	2
2. 按照批准的评估流程/准则对 RFI 和 RFP 进行评估，并维护书面评估证据。核实候选供应商的推荐信。	
3. 选择最契合 RFP 的供应商。记录和传达决定，然后签署合同。	
4. 在采购软件的具体情况下，在合同条款中包括和规定所有各方的权利和义务。这些权利和义务可能包括知识产权的所有权和许可；维护；担保；仲裁程序；升级条款；目的适用性，包括安全、隐私、托管和访问权限。	3
5. 在采购开发资源的具体情况下，在合同条款中包括并规定所有各方的权利和义务。这些权利和义务可能包括知识产权的所有权和许可；目的适用性，包括开发方法；测试；质量管理流程，包括必要的性能衡量准则；性能审查；付款依据；保修；仲裁程序；人力资源管理；以及企业政策的遵守。	
6. 就知识产权所有权及许可方面的资源开发采购协议进行法律咨询。	
7. 在采购基础设施、设备及相关服务的具体情况下，在合同条款中包括和规定所有各方的权利和义务。这些权利和义务可能包括服务水平、维护程序、访问控制、安全、隐私、性能审查、付款依据和仲裁程序。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO10.03 管理供应商关系与合同。 针对每个供应商规范和管理供应商关系。管理、维护和监控合同与服务交付。确保新的或变更的合同符合企业标准以及法律和监管要求。处理合同争议。	a. 合同中定义有控制要求的第三方供应商的百分比 b. 与供应商发生的正式争议的数量 c. 供应商审查会议的次数 d. 在合理时间内得到友好解决的争议百分比

活动	能力级别
1. 为所有供应商指定关系所有者，并让他们对所提供的服务质量负责。	3
2. 规定正式的沟通和审查流程，包括供应商交互和时间安排。	
3. 与供应商商定、管理、维护和更新正式合同。确保合同符合企业标准以及法律和监管要求。	
4. 在与主要服务供应商签订的合同中，纳入由管理层或独立第三方审查供应商场地和内部实践及控制的条款。商定对提供外包服务的供应商的运营环境进行独立审计和鉴证控制，以确认协定的要求得到充分满足。	
5. 使用既定程序处理合同争议。任何可能的情况下，首先利用有效的关系和沟通来克服服务问题。	
6. 定义和规范每个服务供应商的角色和职责。如果多个供应商联合提供某项服务，可考虑指定其中一个供应商作为总承包商，由其负责整个合同。	
7. 评估关系的有效性并识别必要的改进。	4
8. 定义、沟通并商定实现必要的关系改进的方法。	5

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 20000-1:2011(E)	7.2 Supplier management
ITIL 第 3 版，2011 年	Service Design, 4.8 Supplier Management

A. 组件：流程（续）	
管理实践	**指标示例**
APO10.04 管理供应商风险。 识别和管理与供应商能否持续提供安全、高效、有效的服务交付相关的风险。这还包括与直接供应商交付服务相关的分包商或上游供应商。	a. 与供应商召开风险管理会议的频率 b. 导致服务事故的风险相关事件的数量 c. 妥善解决（时间和成本）的风险相关事故的百分比

活动	能力级别
1. 在拟定合同时，为防范潜在的服务风险，应明确定义服务要求，包括：软件托管协议、备选供应商或备用协议（以规避可能发生的供应商违约风险）；知识产权安全和保护；隐私；以及任何法律或监管要求。	3
2. 识别、监控并在适当情况下管理与供应商高效、有效、安全、保密、可靠和持续交付服务能力的相关风险。与外包服务提供商整合关键的内部 IT 管理流程（例如性能和容量规划、变更管理和配置管理等方面）。	4
3. 评估更大规模的供应商生态系统，识别、监控及在适当情况下管理与分包商和上游供应商相关的风险，这些风险会影响供应商高效、有效、安全、可靠和持续交付服务的能力。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	RM.MP Manage External Participation
ISF, The Standard of Good Practice for Information Security 2016	SC1.1 External Supplier Management Process
ISO/IEC 27002:2013/Cor.2:2015(E)	15. Supplier relationships
美国国家标准与技术研究所，Framework for Improving Critical Infrastructure Cybersecurity，第 1.1 版，2018 年 4 月	D.SC Supply Chain Risk Management

管理实践	指标示例
APO10.05 监控供应商的绩效和合规性。 定期审查供应商的整体绩效、对合同要求的遵循情况以及性价比。解决发现的问题。	a. 供应商导致的 I&T 相关的服务违规数量 b. 满足商定要求的供应商的百分比

活动	能力级别
1. 如有必要，要求对供应商的内部实践和控制开展独立审查。	3
2. 规定和记录用于监控供应商绩效是否符合服务水平协议的准则。确保供应商定期、透明地根据商定准则进行报告。	4
3. 监控和审查服务交付，确保供应商提供合格的服务质量、满足要求并遵守合同条件。	
4. 审查供应商的绩效和性价比。确保与备选供应商和市场情况相比，供应商是可信的而且有竞争力。	
5. 监控和评估关于供应商和供应商供应链的外部渠道信息。	
6. 定期记录和评估审查结果，并与供应商进行讨论，以找出是否有改进需求和改进机会。	5

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构														
关键管理实践	首席风险官	首席信息官	首席技术官	首席数字官	I&T 治理委员会	企业风险委员会	开发总监	IT 运营总监	IT 行政总监	服务经理	信息安全经理	隐私官	法律顾问
APO10.01 确定和评估供应商关系与合同。		R	R	R	A				R				R
APO10.02 选择供应商。		R	R	R	A		R	R	R	R	R	R	
APO10.03 管理供应商关系与合同。		R	R	R	A		R	R	R	R			R
APO10.04 管理供应商风险。	R	R	R	R	A	R	R	R	R	R	R	R	
APO10.05 监控供应商的绩效和合规性。	R	R	R	R	A	R	R	R	R	R			R

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
APO10.01 确定和评估供应商关系与合同。	在 COBIT 外部	供应商合同	供应商目录	BAI02.02
			供应商合同的潜在修订	内部
			供应商重要性和评估准则	内部
APO10.02 选择供应商。	BAI02.02	高层采购/开发计划	供应商 RFI 和 RFP	BAI02.01；BAI02.02
			RFI 和 RFP 评估	BAI02.02
			供应商评估的决策结果	供应商评估 BAI02.02；EDM04.01
APO10.03 管理供应商关系与合同。	BAI03.04	已批准的采购计划	结果和建议的改进	内部
			沟通和审查流程	内部
			供应商角色和职责	内部
APO10.04 管理供应商风险。	APO12.04	• 面向利益相关方的风险分析和风险概况报告 • 第三方风险评估的结果	识别的供应商交付风险	APO12.01；APO12.03；BAI01.01；BAI11.01
			确定的旨在最小化风险的合同要求	内部
APO10.05 监控供应商的绩效和合规性。			供应商合规性监控准则	内部
			供应商合规性监控审查结果	MEA01.03

C. 组件：信息流和信息项（另请参阅第 3.6 节）（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
本组件没有相关指南	

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
合同管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework，2016 年	D. Enable—D.8. Contract Management
合同管理	Skills Framework for the Information Age，第 6 版，2015 年	ITCM
购买	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	D. Enable—D.4. Purchasing
采购	Skills Framework for the Information Age，第 6 版，2015 年	SORC

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
IT 采购政策	概述采购 IT 硬件、软件和托管解决方案的原则和流程。详述操作系统、计算机网络、硬件规格等标准。提供合同管理指南（例如条款和条件、合同监控）。		
第三方 IT 服务交付管理政策	设定第三方服务相关风险的管理准则。建立行为期望框架，并规定第三方服务提供商在管理与所提供服务相关的风险时必须采取的安全预防措施。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
构建和管理供应商生态系统，以帮助组织进行数字化转型和创新。持续审视环境，搜寻新的、有效的合作伙伴。		
管理层在与供应商沟通时设定基调，并举例说明正确的行为，以协商并实施必要的改进。确保合同符合企业标准以及法律和监管要求。		

G. 组件：服务、基础设施和应用程序
• 合同管理系统 • 第三方鉴证服务

领域：调整、规划和组织 管理目标：APO11 — 妥当管理的质量	焦点领域：COBIT 核心模型

描述

在所有流程、程序和相关企业成果中定义和沟通质量要求。在持续改进和提高效率的过程中，实施控制、持续监控并运用经过验证的实践和标准。

目的

确保以一致的方式交付技术解决方案和服务，以满足企业的质量要求和利益相关方的需求。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG04 财务信息的质量 • EG07 管理信息的质量 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	• AG09 在预算内按时交付计划且满足要求和质量标准 • AG10 I&T 管理信息的质量

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG09	a. 在预算内按时交付的计划/项目的数量 b. 因质量缺陷需要重大返工的计划的数量 c. 对计划/项目质量满意的利益相关方的百分比
EG04	a. 有关企业财务信息的透明度、了解度和准确性的关键利益相关方满意度调查 b. 不遵守财务相关法规的成本	AG10	a. 考虑到可用资源，用户对 I&T 相关管理信息的质量、及时性和可用性的满意度水平 b. 主要因 I&T 相关信息错误或不可用导致的错误业务决策的比率和程度 c. 满足质量准则的信息的百分比
EG07	a. 董事会和执行管理层对决策信息的满意度 b. 基于不准确信息的错误业务决策所导致的事故数量 c. 为有效业务决策提供支持性信息所花的时间 d. 管理信息的及时性		
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比		

A. 组件：流程	
管理实践	**指标示例**
APO11.01 建立质量管理系统 (QMS)。 建立和维护质量管理系统(QMS)，以提供标准、正式且持续的信息质量管理方法。QMS 应使技术和业务流程与业务需求和企业质量管理保持一致。	a. 质量管理审查有效性的百分比 b. 关键利益相关方对质量管理审查计划的满意度百分比

活动	能力级别
1. 确保 I&T 控制框架以及业务流程和 IT 流程均包含与企业要求协调一致的正式且持续的标准质量管理方法。在 I&T 控制框架以及业务流程和 IT 流程中，确定质量要求和衡量准则（例如，基于法律要求和客户要求）。	3
2. 定义组织结构中的质量管理角色、任务、决策权和职责。	
3. 征求管理层和内外部利益相关方在定义质量要求和质量管理准则方面的意见。	
4. 根据商定的验收准则，定期监控和审查 QMS。纳入客户、用户和管理层的反馈。	4
5. 对审查结果中存在的差异做出响应，持续改进 QMS。	5

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 8.1 Plan quality management

管理实践	指标示例
APO11.02 以客户为质量管理的中心。 确定客户要求并确保将其纳入质量管理实践，做到以客户为质量管理的中心。	a. 客户满意度百分比 b. 在整个业务及 IT 组织中得到传达的客户要求和期望的百分比

活动	能力级别
1. 确定内外部客户要求并确保 I&T 标准及实践与其保持一致，做到以客户为质量管理的中心。定义和传达有关解决用户/客户与 IT 组织之间冲突的角色和职责。	3
2. 管理每个业务流程、IT 运营服务和新解决方案的业务需求和期望。维护它们的质量验收准则。	
3. 在整个业务及 IT 组织中传达客户的要求和期望。	
4. 定期征求客户在业务流程、服务提供和 IT 解决方案交付方面的评价。确定对 I&T 标准和实践的影响，并确保客户期望得到满足和执行。	4
5. 获取质量验收准则以纳入 SLA 中。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
APO11.03 管理质量标准、实践和程序，并将质量管理整合到关键流程和解决方案中。 识别和维护针对关键流程的标准、程序和实践，引导企业达到商定的质量管理标准(QMS) 目标。此活动应符合 I&T 控制框架要求。可考虑针对关键流程、组织部门、产品或服务的认证。	a. 定义了质量要求的流程的数量 b. 在生产前发现的缺陷数量 c. 具有正式质量管理计划的服务数量 d. 包含质量验收标准的 SLA 的数量

A. 组件：流程（续）	
活动	**能力级别**
1. 根据 I&T 控制框架的要求以及企业质量管理准则和政策，定义质量管理标准、实践和程序。	2
2. 在整个组织的关键流程和解决方案中整合所需的质量管理实践。	3
3. 考虑质量认证带来的效益与成本。	
4. 有效传达质量管理方法（例如，通过定期、正式的质量培训计划）。	
5. 记录和监控质量数据。在改进和定制企业质量实践时，参考行业良好实践。	4
6. 定期审查特定质量管理流程的持续相关性、效率及有效性。监控质量目标的实现情况。	
相关指南（标准、框架、合规性要求）	**详细参考**
PMBOK Guide，第 6 版，2017 年	Part 1: 8.2 Manage quality
管理实践	**指标示例**
APO11.04 执行质量监控、控制和审查。 按照质量管理标准，持续监控流程和服务的质量。定义、计划和实施衡量标准来监控客户对质量的满意度，以及质量管理系统 (QMS) 提供的价值。流程所有者应使用收集的信息来提高质量。	a. 已交付的具备正式认证的解决方案和服务的百分比 b. 利益相关方对解决方案和服务的平均满意度评级 c. 具有正式质量评估报告的流程数量 d. 经审查达到质量目的和目标的项目的百分比 e. 风险分析的次数、稳健性和及时性
活动	**能力级别**
1. 为关键组织流程和解决方案准备和开展质量审查。	3
2. 针对这些关键组织流程和解决方案，监控符合总体质量目标的目标驱动型质量指标。	4
3. 确保管理层和流程所有者定期根据定义的质量指标来审查质量管理绩效。	
4. 分析总体质量管理绩效结果。	
5. 报告质量管理绩效审查结果，并在适当情况下发起改进工作。	5
相关指南（标准、框架、合规性要求）	**详细参考**
PMBOK Guide，第 6 版，2017 年	Part 1: 8.3 Control quality
管理实践	**指标示例**
APO11.05 维护持续改进。 维护并定期沟通促进持续改进的整体质量计划。该计划应定义要持续改进的需求及其效益。收集并分析关于质量管理系统 (QMS) 的数据，并提高其有效性。纠正不符合要求的情况，防止再次发生。	a. 执行根本原因分析的次数 b. 按时完成的服务和产品的百分比
活动	**能力级别**
1. 建立平台来分享良好实践和捕获关于缺陷和错误的信息，以便从中学习。	2
2. 找出能够使其他服务或项目受益的出色的质量交付流程的例子。将这些例子与服务和项目交付团队分享，鼓励他们改进。	3
3. 找出质量缺陷频发的例子。确定其根本原因，评估其影响和结果，并与服务和/或项目交付团队对改进措施达成一致。	
4. 为员工提供关于持续改进方法和工具的培训。	
5. 根据内部历史数据、行业指南、来自同类企业的标准和数据，对质量审查的结果进行基准检测。	4
相关指南（标准、框架、合规性要求）	**详细参考**
美国国家标准与技术研究所，Framework for Improving Critical Infrastructure Cybersecurity，第 1.1 版，2018 年 4 月	DE.DP Detection Processes

B. 组件：组织结构																				
关键管理实践	首席运营官	首席风险官	首席信息官	首席技术官	首席数字官	I&T 治理委员会	业务流程所有者	组合经理	计划经理	项目经理	项目管理办公室	数据管理职能部门	架构总监	开发总监	IT 运营总监	IT 行政总监	服务经理	信息安全经理	业务连续性经理
APO11.01 建立质量管理系统 (QMS)。	A		R		R											R	R		
APO11.02 以客户为质量管理的中心。			A		R		R										R		
APO11.03 管理质量标准、实践和程序，并将质量管理整合到关键流程和解决方案中。			A	R	R		R	R	R	R	R	R	R	R	R	R	R	R	R
APO11.04 执行质量监控、控制和审查。		R	A		R	R	R										R		
APO11.05 维护持续改进。			A				R	R	R	R	R		R	R	R	R	R	R	R

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
APO11.01 建立质量管理系统 (QMS)。	在 COBIT 外部	企业级质量系统	质量管理系统 (QMS) 角色、职责和决策权	APO01.05；DSS06.03
			质量管理计划	APO14.04；APO14.06；BAI01.07；BAI11.05
			QMS 有效性审查的结果	BAI03.06
APO11.02 以客户为质量管理的中心。	在 COBIT 外部	业务和客户的质量要求	客户对质量管理的要求	APO08.05；APO09.03；BAI01.07；BAI11.06
			服务质量的结果，包括客户反馈	APO08.05；APO09.05；BAI05.01；BAI07.07
			验收准则	BAI02.01；BAI02.02

C. 组件：信息流和信息项（另请参阅第 3.6 节）（续）				
管理实践	输入		输出	
	自	描述	描述	至
APO11.03 管理质量标准、实践和程序，并将质量管理整合到关键流程和解决方案中。	BAI02.04	已批准的质量审查	质量管理标准	所有 APO；所有 BAI；所有 DSS；所有 MEA
	在 COBIT 外部	• 现有质量认证 • 行业良好实践	交付质量失败的根本原因	APO08.02；APO09.04；BAI07.08；MEA02.04；MEA04.04
			质量监控的结果	APO08.05；APO09.04；BAI07.08
APO11.04 执行质量监控、控制和审查。	BAI03.06	• 质量保证计划 • 质量审查结果、异常和纠正措施	流程服务质量目标和指标	所有 APO；所有 BAI；所有 DSS；所有 MEA
	DSS02.07	• 事故状态和趋势报告 • 请求履行状态和趋势报告	质量审查和审计的结果	APO08.05；APO09.04；APO09.05；BAI07.08
APO11.05 维护持续改进。			质量审查基准指标结果	所有 APO；所有 BAI；所有 DSS；所有 MEA
			需要分享的良好实践示例	所有 APO；所有 BAI；所有 DSS；所有 MEA
			关于持续改进和最佳实践的沟通	所有 APO；所有 BAI；所有 DSS；所有 MEA

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 8. Project quality management: Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
ICT 质量战略制定	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	D. Enable—D.2. ICT Quality Strategy Development
质量保证	Skills Framework for the Information Age，第 6 版，2015 年	QUAS
质量管理	Skills Framework for the Information Age，第 6 版，2015 年	QUMG
质量标准	Skills Framework for the Information Age，第 6 版，2015 年	QUST

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
质量管理政策	描述管理层的企业质量目标愿景、可接受的质量水平，以及特定团队和实体在确保质量方面的职责。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
推崇质量和持续改进的文化。维护并定期沟通关于质量和持续改进的需求和效益。		

G. 组件：服务、基础设施和应用程序
• QMS • 第三方质量保证服务

领域：调整、规划和组织 管理目标：APO12 — 妥当管理的风险	焦点领域：COBIT 核心模型

描述

持续识别、评估 I&T 相关风险，并将该风险降低到企业执行管理层设定的风险容忍水平以内。

目的

将 I&T 相关企业风险管理整合到总体企业风险管理 (ERM) 中，并平衡 I&T 相关企业风险管理的成本和效益。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG02 妥当管理的业务风险 • EG06 业务服务连续性和可用性	• AG02 妥当管理的 I&T 相关风险 • AG07 信息、参与执行的基础设施和应用程序的安全，以及隐私的安全
企业目标的指标示例	**一致性目标的指标示例**
EG02 a. 风险评估涵盖的关键业务目标和服务的百分比 b. 风险评估未发现的重大事故数量与总事故数量的比率 c. 风险概况的更新频率	AG02 a. 风险概况的更新频率 b. 涵盖 I&T 相关风险的企业风险评估的百分比 c. 风险评估中未识别的 I&T 相关重大事故的数量
EG06 a. 导致重大事故的客户服务或业务流程中断的次数 b. 事故的业务成本 c. 因计划外服务中断而损失的业务处理小时数 d. 与承诺的服务可用性目标有关的投诉百分比	AG07 a. 导致财务损失、业务中断或公众形象受损的保密性事故的数量 b. 导致财务损失、业务中断或公众形象受损的可用性事故的数量 c. 导致财务损失、业务中断或公众形象受损的完整性事故的数量

A. 组件：流程

管理实践	指标示例
APO12.01 收集数据。 识别和收集相关数据，以便能够进行有效的 I&T 相关风险识别、分析和报告。	a. 已在贮存库中捕获关键特征的丢失事件的数量 b. 已在贮存库中捕获的审计、事件和趋势的百分比 c. 存在已知问题的关键系统的百分比

活动	能力级别
1. 确立并维护 I&T 风险相关数据的收集、分类和分析方法。	2
2. 记录关于企业内外部运营环境的重要且相关的 I&T 风险数据。	
3. 采用或定义一种风险分类法，以便对风险场景和影响及可能性类别进行一致的定义。	3
4. 按照风险分类法中定义的影响类别，记录已导致或可能导致业务影响的风险事件的相关数据。从相关事件、事故、问题和调查中捕获相关数据。	
5. 通过基于行业的事件日志、数据库以及关于公共事件披露的行业协议，调查和分析来自外部可用数据和趋势及行业同行的历史 I&T 风险数据和损失经验。	4
6. 对于相似类别的事件，整理收集到的数据并重点关注促成因素。确定多个事件的共同促成因素。	
7. 确定在风险事件发生时存在或不存在的特定条件，以及这些条件对事件发生频率和损失程度的影响方式。	
8. 定期进行事件和风险因素分析，识别新出现的风险事件，并了解相关的内外部风险因素。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Supporting Processes - Risk Management
COSO Enterprise Risk Management，2017 年 6 月	8. Performance—Principle 10
ISO/IEC 27005:2011(E)	8.2 Risk identification; 12. Information security risk monitoring and review
美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	3.1 Preparation (Task 7)

A. 组件：流程（续）	
管理实践	**指标示例**
APO12.02 分析风险。 针对实际I&T 风险提出有据可依的观点，以支持风险决策。	a. 已识别的 I&T 风险场景的数量 b. 自上次更新 I&T 风险场景以来的时间

活动	能力级别
1. 考虑所有风险因素和/或资产的业务关键性，定义适当的风险分析工作范围。	3
2. 构建并定期更新 I&T 风险场景、I&T 相关的损失敞口，以及关于声誉风险的场景（包括级联和/或巧合威胁类型与事件的复合场景）。为待检测的特定控制活动和能力设定期望值。	
3. 评估与 I&T 风险场景相关的损失或收益的发生频率（或可能性）和程度。考虑所有适用的风险因素，并评估已知的运营控制。	
4. 将当前风险（I&T 相关的损失敞口）与风险偏好和可接受的风险容忍度进行比较。识别不可接受的或上升的风险。	
5. 对超过风险偏好和容忍度的风险提出风险应对建议。	
6. 为将实施所选风险应对措施的项目或计划指定高层次要求。确定风险缓解应对措施中的适当关键控制的要求和期望。	
7. 在参考风险分析和业务影响分析 (BIA) 结果制定决策之前，首先对这些结果进行验证。确认分析与企业要求相一致，并验证已对评估结果进行了适当的校正和检查以排除偏差。	4
8. 分析可选的潜在风险应对方案（例如规避、降低/缓解、转移/分摊以及接受和利用等）的成本/效益。确认最佳的风险应对方案。	5

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Supporting Processes—Risk Management
COSO Enterprise Risk Management，2017 年 6 月	8. Performance—Principle 11
ISF, The Standard of Good Practice for Information Security 2016	IR2.1 Risk Assessment Scope; IR2.2 Business Impact Assessment
ISO/IEC 27001:2013/Cor.2:2015(E)	8.2 Information security risk assessment
ISO/IEC 27005:2011(E)	8.3 Risk analysis
美国国家标准与技术研究所，Framework for Improving Critical Infrastructure Cybersecurity，第 1.1 版，2018 年 4 月	ID. RA Risk Assessment
美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	3.6 Authorization (Task 3)
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.17 Risk assessment (RA-3)

管理实践	指标示例
APO12.03 维护风险概况。 维护已知风险和风险属性的清单，包括预期的频率、潜在影响和应对措施。记录与风险项目相关的资源、能力和当前的控制活动。	a. 风险概况中的属性和值的完整性 b. 风险概况中包含的关键业务流程的百分比

活动	能力级别
1. 创建业务流程的清单，并记录它们对 I&T 服务管理流程和 IT 基础设施资源的依赖性。确定支持人员、应用程序、基础设施、设施、关键手册记录、供应商、提供商和外包商。	2
2. 确定并对哪些 I&T 服务和 IT 基础设施资源对于维持业务流程的运作必不可少达成一致。分析依赖关系并识别薄弱环节。	
3. 按类别、业务线和职能领域汇总当前风险场景。	
4. 定期捕获所有风险概况信息，并将其整合为汇总的风险概况。	3
5. 捕获风险行动计划的状态信息，以便将其纳入企业的 I&T 风险概况中。	
6. 根据全部风险概况数据，定义一组风险指标，以实现快速识别和监控当前风险和风险趋势。	4
7. 捕获关于已存在的 I&T 风险事件的信息，以便将其纳入企业的 IT 风险概况中。	

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI Cybermaturity Platform，2018 年	RS.DT Define Organizational Risk Tolerance
COSO Enterprise Risk Management，2017 年 6 月	8. Performance—Principle 12
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.17 Risk assessment (RA-7)
管理实践	**指标示例**
APO12.04 阐明风险。 及时向所有必要的利益相关方传达 I&T 相关敞口和机遇的当前状态信息，以便其做出适当的应对。	a. 利益相关方对所提供的风险报告的满意度水平 b. 风险概况报告的完整性（包括符合利益相关方要求的信息） c. 在制定管理决策时使用风险报告
活动	**能力级别**
1. 使用有利于支持企业决策的术语和格式，向所有受影响的利益相关方报告风险分析结果。在任何可能的情况下，包含损失或收益的发生概率和范围及置信水平，以便管理层能够平衡风险与回报。	3
2. 根据风险分类法，帮助决策者了解最坏情形和最可能的场景、I&T 相关的损失敞口以及重要的声誉、法律和监管考虑因素，或任何其他影响类别。	
3. 向所有利益相关方报告当前的风险概况。包含以下相关信息：风险管理流程的有效性、控制有效性、差距、不一致、冗余、补救状态以及它们对风险概况的影响。	
4. 对于具有相对风险且风险承受能力对等的领域，定期识别允许接受更大风险和促进增长及回报的 I&T 相关的机会。	
5. 审查第三方客观评估和内部审计及质量保证审查的结果。将其纳入风险概况中。审查已识别的差距和 I&T 相关损失敞口，确定是否需要进行额外的风险分析。	4
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI Cybermaturity Platform，2018 年	RS.CR Determine Critical Infrastructure Requirements
COSO Enterprise Risk Management，2017 年 6 月	10. Information, Communication, and Reporting—Principle 19
ISO/IEC 27005:2011(E)	11. Information security risk communication and consultation
美国国家标准与技术研究所，Framework for Improving Critical nfrastructure Cybersecurity，第 1.1 版，2018 年 4 月	ID.RM Risk Management Strategy
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.15 Program management (PM-32)
管理实践	**指标示例**
APO12.05 定义风险管理行动组合。 以组合形式管理各种能将风险降至可接受水平的机会。	a. 风险管理组合中没有识别和包含的重大事故的数量 b. 因未充分考虑其他相关风险而被拒绝的风险管理项目提议的百分比
活动	**能力级别**
1. 维护控制活动的清单，实施这些控制活动是为了缓解风险，并使将要承担的风险符合风险偏好和容忍度。对控制活动进行分类，并将其与特定的 I&T 风险场景和汇总的 I&T 风险场景相匹配。	2
2. 确定每个组织实体是否监控风险，并接受在其单独和组合容忍度以内的风险运营责任。	3
3. 在考虑成本、效益、对当前风险概况的影响和监管要求的前提下，定义一组平衡的项目建议（旨在降低风险）和/或项目（支持企业战略机会）。	
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI 数据管理成熟度模型，2014 年	Supporting Processes—Risk Management
COSO Enterprise Risk Management，2017 年 6 月	8. Performance—Principle 14
HITRUST CSF，第 9 版，2017 年 9 月	03.01 Risk Management Program

A. 组件：流程（续）	
管理实践	**指标示例**
APO12.06 应对风险。 及时对发生的风险事件作出应对，采取有效措施控制损失程度。	a. 未能降低剩余风险的措施数量 b. 按设计执行的 I&T 风险行动计划的百分比

活动	能力级别
1. 制定、维护和测试相关计划，其中记录当风险事件可能导致重大运营或开发事故并产生严重的业务影响时应采取的具体步骤。确保此等计划包含在整个企业的上报路径。	3
2. 应用适当的风险应对计划，尽可能减小风险事故发生时产生的影响。	
3. 将事故分类，并将 I&T 相关的损失风险敞口与风险容忍度阈值进行比较。在报告中向决策者说明事故产生的业务影响，并更新风险概况。	4
4. 检查过去的不良事件/损失和错失的机会，并确定根本原因。	
5. 将根本原因、其他风险应对要求和流程改进告知相应的决策者。确保将原因、应对要求和流程改进纳入风险治理流程中。	5

相关指南（标准、框架、合规性要求）	详细参考
COSO Enterprise Risk Management，2017 年 6 月	8. Performance—Principle 13
ISF, The Standard of Good Practice for Information Security 2016	IR2.9 Risk Treatment
ISO/IEC 27001:2013/Cor.2:2015(E)	6.1 Action to address risk and opportunities
ISO/IEC 27005:2011(E)	9. Information security risk treatment
美国国家标准与技术研究所特别出版物 800-37， 修订版 2（草稿），2018 年 5 月	3.6 Authorization (Task 4)
美国国家标准与技术研究所特别出版物 800-53， 修订版 5（草稿），2017 年 8 月	3.15 Program management (PM-9, PM-31)

B. 组件：组织结构																		
关键管理实践	首席风险官	首席信息官	首席技术官	首席数字官	企业风险委员会	首席信息安全官	业务流程所有者	项目管理办公室	数据管理职能部门	架构总监	开发总监	IT 运营总监	IT 行政总监	服务经理	信息安全经理	业务连续性经理	隐私官
APO12.01 收集数据。	A	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
APO12.02 分析风险。	A	R			R		R										
APO12.03 维护风险概况。	A	R			R		R										
APO12.04 阐明风险。	A	R			R		R										
APO12.05 定义风险管理行动组合。	A	R			R		R										
APO12.06 应对风险。	R	A	R	R		R	R	R		R	R	R	R	R	R	R	R

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-37，修订版 2， 2017 年 9 月	3.1 Preparation (Task 1); Appendix A: Roles and Responsibilities

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
APO12.01 收集数据。	APO02.02	当前能力存在的相关差距和风险	新出现的风险问题和因素	APO01.01；APO02.02；EDM03.01
	APO02.05	风险评估举措	风险事件和促成因素的相关数据	内部
	APO10.04	识别的供应商交付风险	与风险有关的运营环境相关数据	内部
	DSS02.07	事故状态和趋势报告		
	EDM03.01	风险管理活动的评估		
	EDM03.02	• 风险管理政策 • 风险管理的主要监控目标 • 已批准的风险管理衡量流程		
APO12.02 分析风险。	DSS04.02	业务影响分析 (BIA)	风险分析结果	APO01.01；APO02.02；EDM03.03；BAI01.08；BAI11.06
	DSS05.01	潜在威胁的评估	I&T 风险场景	内部
	在 COBIT 外部	威胁公告	风险分析工作的范围	内部
APO12.03 维护风险概况。	APO10.04	识别的供应商交付风险	汇总的风险概况，包括风险管理行动的状态	APO02.02；EDM03.02
	DSS05.01	潜在威胁的评估	按业务线和职能记录的风险场景	内部
	EDM03.01	• 风险偏好的指导准则 • 已批准的风险容忍度水平		
APO12.04 阐明风险。			面向利益相关方的风险分析和风险概况报告	APO10.04；EDM03.03；EDM05.02；MEA04.05
			第三方风险评估的结果	APO10.04；EDM03.03；MEA02.01
			接受更高风险的机会	EDM03.03

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
APO12.05 定义风险管理行动组合。	**自**	**描述**	**描述**	**至**
			旨在降低风险的项目建议	APO02.02; APO13.02
APO12.06 应对风险。	EDM03.03	解决风险管理偏离的补救措施	风险影响的沟通	APO01.02; APO08.04; DSS04.02
			风险相关的根本原因	DSS02.03; DSS03.01; DSS03.02; DSS03.03; DSS03.05; DSS04.02; MEA02.04; MEA04.04; MEA04.06
			风险相关事故的应对计划	DSS02.05

相关指南（标准、框架、合规性要求）	详细参考
COSO Enterprise Risk Management，2017 年 6 月	10. Information, Communication, and Reporting—Principle 20
SF, The Standard of Good Practice for Information Security 2016	IR1.3 Information Risk Assessment—Supporting Material
美国国家标准与技术研究所特别出版物 800-37，修订版 2，2017 年 9 月	3.1 Preparation (Task 7): Inputs and Outputs; 3.6 Authorization (Task 3, 4): Inputs and Outputs
PMBOK Guide，第 6 版，2017 年	Part 1: 11. Project risk management: Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
业务风险管理	Skills Framework for the Information Age，第 6 版，2015 年	BURM
信息鉴证	Skills Framework for the Information Age，第 6 版，2015 年	INAS
风险管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage—E.3. Risk Management

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
企业风险政策	在战略、策略和运营层面定义与业务目标一致的企业风险治理和管理。将企业治理转化为风险治理原则和政策，并详细阐述风险管理活动。	美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.17 Risk assessment (RA-1)
欺诈风险政策	规定当因欺诈或行为不当而造成损失或损害时，应保护企业品牌、声誉和资产。指导员工报告可疑活动和处理敏感信息及证据。鼓励反欺诈文化并培养风险意识。	美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
为支持透明的参与式风险文化，高级管理层应该为在整个企业中推行风险实践设定方向，并展现出明确、有力的支持。管理层应鼓励对 I&T 相关的业务风险公开进行沟通并确立业务所有权。理想的行为包括调整政策以符合定义的风险偏好、向高级管理层和风险治理机构报告风险趋势、奖励有效的风险管理，以及积极监控风险和风险行动计划的进展。	ISF, The Standard of Good Practice for Information Security 2016	IR1.2 Information Risk Assessment

G. 组件：服务、基础设施和应用程序
• 危机管理服务 • 治理、风险与合规性 (GRC) 工具 • 风险分析工具 • 风险情报服务

领域：调整、规划和组织 管理目标：APO13 — 妥当管理的安全	焦点领域：COBIT 核心模型

描述

确定、运营和监控信息安全管理系统。

目的

确保将信息安全事故的发生和影响保持在企业的风险偏好水平内。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG02 妥当管理的业务风险 • EG06 业务服务连续性和可用性	AG07 信息、参与执行的基础设施和应用程序的安全，以及隐私的安全

企业目标的指标示例	
EG02	a. 风险评估涵盖的关键业务目标和服务的百分比 b. 风险评估未发现的重大事故数量与总事故数量的比率 c. 风险概况的更新频率
EG06	a. 导致重大事故的客户服务或业务流程中断的次数 b. 事故的业务成本 c. 因计划外服务中断而损失的业务处理小时数 d. 与承诺的服务可用性目标有关的投诉百分比

一致性目标的指标示例	
AG07	a. 导致财务损失、业务中断或公众形象受损的保密性事故的数量 b. 导致财务损失、业务中断或公众形象受损的可用性事故的数量 c. 导致财务损失、业务中断或公众形象受损的完整性事故的数量

A. 组件：流程

管理实践	指标示例
APO13.01 建立和维护信息安全管理系统 (ISMS)。 建立并维护一套信息安全管理系统 (ISMS)，为信息安全管理提供一种标准、正式和连续的方法，实现与业务需求一致的安全技术和业务流程。	a. 利益相关者对整个企业范围内安全计划的满意度

活动	能力级别
1. 根据企业、组织、所在位置、资产和技术的特征确定信息安全管理系统 (ISMS) 的范围和边界。列明该范围的任何排除项的详细信息和排除理由。	2
2. 根据企业政策和企业的运营环境确定 ISMS。	
3. 确保 ISMS 与企业的总体安全管理方法保持一致。	
4. 获得实施以及运行或更改 ISMS 的管理授权。	
5. 制定并维护旨在描述 ISMS 范围的适用性声明。	
6. 定义和传达信息安全管理的角色和职责。	
7. 传达 ISMS 方法。	

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
HITRUST CSF，第 9 版，2017 年 9 月	0.01 Information Security Management program
ISO/IEC 20000-1:2011(E)	6.6 Information security management
ITIL 第 3 版，2011 年	Service Design, 4.7 Information Security Management
美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	3.3 Selection (Task 1); 3.4 Implementation (Task 1)
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.17 Risk assessment (RA-2)
管理实践	**指标示例**
APO13.02 确定和管理信息安全和隐私风险处置计划。 维护旨在说明如何管理信息安全风险并使其符合企业战略和企业架构的信息安全计划。确保安全改进实施建议以认可的业务案例为基础，并作为服务和解决方案开发的有机组成部分实施，然后作为业务运营的有机组成部分来运作。	a. 安全风险场景模拟的成功率 b. 成功完成信息安全意识培训的员工人数

活动	**能力级别**
1. 制定并维护符合战略目标和企业架构的信息安全风险处置计划。确保计划确定了适当和最优的管理实践和安全解决方案，以及用于管理已识别的信息安全风险的相关资源、职责和优先级。	3
2. 作为企业架构的一部分，维护已实施的用于管理安全相关风险的解决方案组件清单。	
3. 制定实施信息安全风险处置计划的建议，并以恰当的业务案例为支持，包括考虑资金、角色和责任的分配。	
4. 为从信息安全风险处置计划中选择的管理实践和解决方案的设计和开发提供意见。	
5. 开展信息安全与隐私的培训和意识计划。	
6. 将信息安全和隐私程序的计划、设计、实施和监控与其他能够实现快速预防和检测安全事件以及应对安全事故的控制措施进行整合。	
7. 确定如何衡量所选管理实践的有效性。具体说明如何使用这些衡量指标来评估有效性，从而生成可比较且可重复的结果。	4

相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	
管理实践	**指标示例**
APO13.03 监控和审查信息安全管理系统 (ISMS)。 维护并定期沟通关于信息安全持续改进的需求和效益。收集并分析关于信息安全管理系统 (ISMS) 的数据，并提高其有效性。纠正不符合要求的情况，防止再次发生。	a. 计划内安全审查的频率 b. 计划内定期安全审查所获发现的数量 c. 利益相关方对安全计划的满意度 d. 因未遵守安全计划而导致的安全相关事故的数量

A. 组件：流程（续）	
活动	**能力级别**
1. 对 ISMS 的有效性进行定期审查。包括是否符合 ISMS 政策和目标，以及审查安全和隐私实践。	4
2. 按照计划的时间间隔进行 ISMS 审计。	
3. 定期对 ISMS 进行管理审查，确保其保持充分的范围，并识别 ISMS 流程中的改进。	
4. 记录可能影响 ISMS 的有效性或绩效的行动和事件。	
5. 针对安全计划的维护提供意见，并将监控和审查活动的结果考虑在内。	5
相关指南（标准、框架、合规性要求）	**详细参考**
美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	3.3 Selection (Task 3)

B. 组件：组织结构															
关键管理实践	**首席信息官**	**首席技术官**	**企业风险委员会**	**首席信息安全官**	**业务流程所有者**	**项目管理办公室**	**架构总监**	**开发总监**	**IT 运营总监**	**IT 行政总监**	**服务经理**	**信息安全经理**	**业务连续性经理**	**隐私官**
APO13.01 建立和维护信息安全管理系统 (ISMS)。	R		R	A						R		R		
APO13.02 确定和管理信息安全和隐私风险处置计划。	R		R	A						R		R		R
APO13.03 监控和审查信息安全管理系统 (ISMS)。	R	R		A	R	R	R	R	R	R	R	R	R	R
相关指南（标准、框架、合规性要求）	**详细参考**													
ISF, The Standard of Good Practice for Information Security 2016	SG1.2 Security Direction													
ISO/IEC 27002:2013/Cor.2:2015(E)	6.1 Internal organization													

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	**输入**		**输出**	
	自	**描述**	**描述**	**至**
APO13.01 建立和维护信息安全管理系统 (ISMS)。	在 COBIT 外部	企业安全方法	ISMS 范围声明	APO01.05；DSS06.03
			ISMS 政策	内部
APO13.02 确定和管理信息安全风险处置计划。	APO02.04	为实现目标能力需弥补的差距和做出的改变	信息安全风险处置计划	所有 APO；所有 BAI；所有 DSS；所有 MEA；所有 EDM
	APO03.02	基准指标领域说明和架构定义	信息安全业务案例	APO05.02
	APO12.05	旨在降低风险的项目建议		

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	输入		输出	
	自	描述	描述	至
APO13.03 监控和审查信息安全管理系统 (ISMS)。	DSS02.02	已分类并排定优先级的事故和服务请求	旨在改进信息安全管理系统 (ISMS)的建议	内部
			信息安全管理系统 (ISMS) 审计报告	MEA02.01
相关指南（标准、框架、合规性要求）		**详细参考**		
美国国家标准与技术研究所特别出版物 800-37，修订版 2，2017 年 9 月		3.3 Selection (Tasks 1, 3): Inputs and Outputs; 3.4 Implementation (Task 1): Inputs and Outputs		

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
信息安全	Skills Framework for the Information Age，第 6 版，2015 年	SCTY
信息安全战略开发	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework，2016 年	D. Enable—D.1. Information Security Strategy Development

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
信息安全和隐私政策	制定行为准则以保护公司信息、系统和基础设施。鉴于安全和存储方面的业务需求相较于 I&T 风险管理和隐私更具动态性，其治理应与 I&T 风险和隐私管理分开处理。为确保运营效率，需要使信息安全政策与 I&T 风险和隐私政策同步。	(1) ISO/IEC 27001:2013/Cor.2:2015(E)；(2) ISO/IEC 27002:2013/Cor.2:2015(E)；(3) 美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月；(4) HITRUST CSF，第 9 版，2017 年 9 月；(5) ISF，The Standard of Good Practice for Information Security 2016	(1) 5.2 Policy; (2) 5. Information security policies; (3) 3.2 Awareness and training (AT-1); (4) 04.01 Information Security Policy; (5) SM1.1 Information Security Policy

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
建立能对日常实践中安全和隐私政策的理想行为和实际实施产生积极影响的安全和隐私意识文化。提供充分的安全和隐私指导，指明安全和隐私倡导者（包括 C 级高管、人力资源主管以及安全和/或隐私专业人员），并主动支持和传达安全和隐私计划、创新及挑战。	(1) ISO/IEC 27001:2013/Cor.2:2015(E)；(2) Creating a Culture of Security, ISACA, 2011	1) 7.3 意识；(2) 实现主动安全意识文化的框架（所有章节）

G. 组件：服务、基础设施和应用程序
• 配置管理工具 • 安全和隐私意识服务 • 第三方安全评估服务

领域：调整、规划和组织 管理目标：APO14 — 妥当管理的数据	焦点领域：COBIT 核心模型

描述

在整个数据生命周期（从创建到交付、维护和归档）中实现并维持有效的企业数据资产管理。

目的

确保有效利用关键数据资产，以实现企业目标和目的。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG04 财务信息的质量 • EG07 管理信息的质量	AG10 I&T 管理信息的质量

企业目标的指标示例	
EG04	a. 有关企业财务信息的透明度、了解度和准确性的关键利益相关方满意度调查 b. 不遵守财务相关法规的成本
EG07	a. 董事会和执行管理层对决策信息的满意度 b. 基于不准确信息的错误业务决策所导致的事故数量 c. 为有效业务决策提供支持性信息所花的时间 d. 管理信息的及时性

一致性目标的指标示例	
AG10	a. 考虑到可用资源，用户对 I&T 相关管理信息的质量、及时性和可用性的满意度水平 b. 主要因 I&T 相关信息错误或不可用导致的错误业务决策的比率和程度 c. 满足质量准则的信息的百分比

A. 组件：流程

管理实践	指标示例
APO14.01 定义和传达组织的数据管理战略以及角色与职责。 根据企业战略和目标确定如何管理和改进组织的数据资产。向所有利益相关方传达数据管理战略。分配角色和职责，以确保将公司数据作为关键资产进行管理，并以有效且可持续的方式执行和维护数据管理战略。	a. 数据管理违规数量（与既定战略的差距） b. 为支持数据管理治理以及数据管理职能与治理之间的交互而确定的角色和职责的百分比

活动	能力级别
1. 建立数据管理职能，负责管理旨在支持数据管理目标的活动。	2
2. 具体指明用于支持数据管理以及数据管理职能与治理之间的交互的角色和职责。	
3. 确保业务和技术部门合作制定组织的数据管理战略。确保数据管理目标、优先级和范围能反映企业目标，且符合数据管理政策和法规的规定，并得到所有利益相关方的批准。	3
4. 传达数据管理目标、优先级和范围，并根据反馈进行相应调整（视需要而定）。	
5. 利用指标评估和监控数据管理目标的实现情况。	4
6. 监控计划的执行顺序，以实施数据管理战略。根据进度审查结果更新计划（视需要而定）。	
7. 利用统计和其他定量方法评估数据管理的战略目标在实现业务目标方面的有效性。根据指标进行修改（视需要而定）。	
8. 确保组织对创新业务流程和新兴监管要求进行研究，以保证数据管理计划与未来业务需求保持一致。	5
9. 针对数据管理战略的开发与实施，为行业最佳实践做出贡献。	

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI 数据管理成熟度模型，2014 年	Data Management Strategy - Data Management Strategy; Data Governance—Governance Management
ITIL 第 3 版，2011 年	Service Design, 5.2 Management of Data and Information
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 13: Data Protection
管理实践	**指标示例**
APO14.02 定义和维护一致的业务词汇表。 创建、批准、更新和推广一致的业务术语和定义，以促进共享数据在整个组织的使用。	a. 整个组织的业务词汇表术语的接受水平和使用频率 b. 新开发工作中使用的既定业务词汇表术语的同义词数量 c. 既定业务词汇表术语的精细度水平

活动	能力级别
1. 确保标准业务术语易于获取且已传达给相应的利益相关方。	2
2. 确保添加到业务词汇表内的每个业务术语具有唯一的名称和定义。	
3. 在业务词汇表中使用标准行业业务术语和定义（如适用）。	
4. 制定、记录并遵循用于定义、管理、使用和维护业务词汇表的流程。例如，新举措应将标准业务术语作为数据需求定义流程的一部分，以确保措辞的一致性。这将有助于实现内容的可比性，并促进整个组织的数据共享。	3
5. 确保新的开发、数据集成和数据整合工作将标准业务术语作为数据需求定义流程的一部分。	
6. 将业务词汇表集成到组织的元数据贮存库中并提供相应的访问权限。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Data Governance - Business Glossary
ISF, The Standard of Good Practice for Information Security 2016	IM1.1 Information Classification and Handling
管理实践	**指标示例**
APO14.03 建立元数据管理的流程和基础设施。 建立流程和基础设施，具体指明和扩展关于组织数据资产的元数据，促进和支持数据共享，确保数据的合规使用，提高对业务变化的响应能力并降低数据相关风险。	a. 在元数据中识别的错误数量 b. 包含用于评估元数据准确性和采用情况的衡量标准和指标的元数据百分比

活动	能力级别
1. 制定和遵循元数据管理流程。	2
2. 确保元数据文档捕获数据相互依存关系。	
3. 建立和遵循元数据类别、属性和标准。	
4. 开发和使用元数据，对潜在的数据变化进行影响分析。	3
5. 根据分段实施计划，为组织的元数据贮存库填充更多元数据类别和分类。将该贮存库与架构层相关联。	
6. 根据现有架构对元数据和元数据的任何更改进行验证。	
7. 确保组织已开发部署到所有平台的集成元模型。	
8. 确保元数据类型和数据定义支持一致的导入、订阅和使用实践。	
9. 使用衡量标准和指标评估元数据的准确性和采用情况。	4
10. 评估计划内的数据更改对元数据贮存库产生的影响。持续改进元数据的捕获、更改和优化流程。	5

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Data Governance—Metadata Management
ISO/IEC 27002:2013/Cor.2:2015(E)	8.2 Information classification

A. 组件：流程（续）	
管理实践	**指标示例**
APO14.04 制定数据质量战略。 制定整个组织的综合战略，以实现和维护支持业务目标和目的所需的数据质量水平（如复杂性、完整性、准确性、完全性、有效性、可追溯性和及时性）。	a. 在顺序计划中发现和记录的数据质量改进工作的数量 b. 对数据质量满意的利益相关方的百分比

活动	能力级别
1. 与业务和技术利益相关方共同制定数据质量战略，获得执行管理层的批准并进行管理。该战略应有助于从现状转变为目标状态。此外还应与业务目标和组织的数据管理战略保持明确一致。	3
2. 确保整个组织遵循数据质量战略，并配合使用相应的政策、流程和准则。	
3. 确立数据质量战略中包含的跨数据生命周期的政策、流程和治理。在系统开发生命周期方法中强制实施相应的流程。	
4. 制定、监控和维护序列计划，在整个组织开展数据质量改善工作。	
5. 为评估进度，监控计划是否符合数据质量战略的目的和目标。	4
6. 系统地收集利益相关方的数据质量问题报告。数据质量战略中应包含他们对提高数据质量的期望。对报告进行衡量和监控。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	DP.DR Safeguard Data at Rest；DP.DT Safeguard Data in Transit; DP.IP Integrity and Data Leak Prevention
CMMI 数据管理成熟度模型，2014 年	Data Quality - Data Quality Strategy

管理实践	指标示例
APO14.05 建立数据分析方法、流程和工具。 实施可供多个数据贮存库和数据存储使用的标准化数据分析方法、流程、实践、工具和模板。	a. 既定和已实施的数据模板数量及其使用百分比 b. 具有既定数据配置文件的共享数据集数量

活动	能力级别
1. 定义数据分析方法、流程、实践、工具和结果模板并进行标准化。确保分析流程可供多个数据存储和共享数据贮存库重复使用和利用。	3
2. 利用数据管理识别需要定期分析和监控的核心共享数据集。	4
3. 数据分析工作中包括评估数据内容是否符合经批准的元数据和标准。	
4. 在数据分析活动期间，根据历史分析结果将实际问题与统计预测的问题进行比较。	
5. 确保集中存储结果，并在统计数据和指标方面进行系统的监控和分析。提供随时间获得的数据质量改进方面的见解。	
6. 为所有关键数据馈送和贮存库创建实时或近乎实时的自动分析报告。	5

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Data Quality—Data Profiling
美国国家标准与技术研究所特别出版物 800-53，修订版 5，2017 年 8 月	3.20 System and information integrity (SI-1)

管理实践	指标示例
APO14.06 确保数据质量评估方法。 提供系统的方法，根据流程、技术和数据质量规定来衡量和评估数据质量。	a. 在数据质量评估结果中发现的问题数量 b. 包含补救建议的数据质量评估结果的数量

A. 组件：流程（续）	
活动	**能力级别**
1. 根据数据质量评估政策所批准的频率，定期进行数据质量评估。确保数据治理按数据质量评估的主题领域确定关键属性集。	4
2. 数据质量评估结果中包含补救建议及支持依据。	
3. 使用各个选定质量维度的既定阈值和目标对数据质量进行评估。	
4. 根据属性的重要度和数据波动，系统地生成数据质量衡量报告。	
5. 持续审查和改进数据质量评估及报告流程。	5
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI 数据管理成熟度模型，2014 年	Data Quality—Data Quality Assessment
管理实践	**指标示例**
APO14.07 定义数据清理方法。 根据预定义的业务规则确定验证和纠正数据的机制、规则、流程和方法。	a. 数据得到正确清理的百分比 b. 包含数据质量衡量标准且由数据提供者对已清理数据负责的 SLA 百分比
活动	**能力级别**
1. 制定并维护数据清理政策。	2
2. 通过清理活动维护数据更改历史记录。	3
3. 制定纠正数据的方法并在计划中定义这些方法。方法可能包括比较多个贮存库、对照有效来源执行验证、逻辑检验、参照完整性或范围容差。	4
4. 在服务水平协议中，纳入支持数据提供者对已清理数据负责的数据质量标准。	
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI 数据管理成熟度模型，2014 年	Data Quality—Data Cleansing
管理实践	**指标示例**
APO14.08 管理数据资产的生命周期。 确保组织了解、对应、盘存和控制其业务流程在整个数据生命周期（从创建或采购到停用）内的数据流。	a. 无法对应到数据源的数据用户需求数量 b. 共享数据集的数量 c. 距离上次将业务流程对应到数据的合规性检查的时间
活动	**能力级别**
1. 对应并调整数据用户和生产者的需求。	2
2. 定义业务流程到数据的对应关系。维护这些对应关系并定期审查它们是否合规。	3
3. 遵循合作协议中关于业务流程中的共享数据和数据使用的既定流程。	
4. 针对组织层面的各个主要业务流程的共享数据实施数据流和完整的数据到流程生命周期图。	
5. 确保为实现特定业务目的而对共享数据集或目标数据集执行的更改将由数据治理结构进行管理，并且相应的利益相关方也参与其中。	
6. 利用指标来扩展经批准的共享数据重用并消除流程冗余。	4
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI 数据管理成熟度模型，2014 年	Data Operations—Data Lifecycle Management

A. 组件：流程（续）	
管理实践	**指标示例**
APO14.09 支持数据归档和保留。 确保数据维护满足历史数据可用性方面的组织和监管要求。确保符合数据归档和保留方面的法律和监管要求。	a. 尝试将数据传输到归档的失败率 b. 符合历史数据可用性方面的组织和监管要求以及数据归档和保留方面的法律和监管要求的数据维护百分比

活动	能力级别
1. 确保政策强制实施数据历史记录管理，包括保留、销毁和审计轨迹要求。	2
2. 确保现存的既定方法保证可以访问支持业务需求所需的历史数据。	
3. 利用政策和流程对历史数据和归档数据的访问、传输和修改施加控制。	
4. 确保组织具有规定的数据仓库贮存库，并且可借助该贮存库访问历史数据，以满足旨在支持业务流程的分析需求。	3

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Platform and Architecture—Historical Data, Retention and Archiving

管理实践	指标示例
APO14.10 管理数据备份和恢复安排。 管理关键数据的可用性以确保运营连续性。	a. 尝试备份数据的失败率 b. 尝试恢复备份数据的成功率

活动	能力级别
1. 制定计划以确保正确备份所有关键数据。	2
2. 定义备份数据的本地和异地存储要求，确保与业务需求协调一致，同时考虑容量、能力和保留期限。	
3. 为备份数据制定测试计划。确保数据能够正确恢复，并且不会对业务产生重大影响。	

相关指南（标准、框架、合规性要求）	详细参考
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 10: Data Recovery Capability

B. 组件：组织结构

关键管理实践	首席风险官	首席信息官	首席数字官	企业风险委员会	首席信息安全官	数据管理职能部门	法律顾问
APO14.01 定义和传达组织的数据管理战略以及角色与职责。	R	A	R		R	R	
APO14.02 定义和维护一致的业务词汇表。	R	A	R		R	R	
APO14.03 建立元数据管理的流程和基础设施。	R	A	R		R	R	
APO14.04 制定数据质量战略。	R	A	R		R	R	
APO14.05 建立数据分析方法、流程和工具。	R	A	R		R	R	
APO14.06 确保数据质量评估方法。	R	A	R		R	R	
APO14.07 定义数据清理方法。	R	A	R		R	R	
APO14.08 管理数据资产的生命周期。	R	A	R	R	R	R	R
APO14.09 支持数据归档和保留。	R	A	R	R	R	R	R
APO14.10 管理数据备份和恢复安排。	R	A	R		R	R	R

B. 组件：组织结构（*续*）	
相关指南（标准、框架、合规性要求）	**详细参考**
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	**输入**		**输出**	
	自	**描述**	**描述**	**至**
APO14.01 定义和传达组织的数据管理战略以及角色与职责。	APO01.06	数据分类准则	数据管理战略	APO03.02；APO14.10
	APO07.03	技能和能力矩阵	商定的数据管理和数据治理角色及职责	内部
	在 COBIT 外部	• 企业战略 • 数据管理政策和法规	外部出版物和行业会议提供的最佳实践报告	内部
			数据管理战略的实施计划	内部
APO14.02 定义和维护一致的业务词汇表。			业务词汇表	APO14.03；BAI02.01
APO14.03 建立元数据管理的流程和基础设施。	APO03.02	信息架构模型	元数据文档	APO03.02
	APO14.02	业务词汇表		
APO14.04 制定数据质量战略。	APO01.06	数据完整性程序	数据质量战略	APO14.05；APO14.06；APO14.07
	APO01.07	数据安全和控制准则	数据质量问题报告	内部
	APO11.01	质量管理计划	数据质量改进计划	内部
APO14.05 制定数据分析方法、流程和工具。	APO14.04	数据质量战略	数据分析方法、流程、实践、工具和结果模板	内部
APO14.06 确保数据质量评估方法。	APO11.01	质量管理计划	数据质量评估结果	内部
	APO14.04	数据质量战略		
APO14.07 定义数据清理方法。	APO14.04	数据质量战略	数据质量要求	APO09.03
APO14.08 管理数据资产的生命周期。	APO01.07	数据安全和控制准则		
	DSS04.07	备份数据		
APO14.09 支持数据归档和保留。	DSS06.05	保留要求	数据归档	内部
APO14.10 管理数据备份和恢复安排。	APO01.07	数据安全和控制准则	备份测试计划	DSS04.07
	APO14.01	数据管理战略	备份计划	DSS04.07
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
数据分析	Skills Framework for the Information Age，第 6 版，2015 年	DTAN
数据管理	Skills Framework for the Information Age，第 6 版，2015 年	DATM
信息鉴证	Skills Framework for the Information Age，第 6 版，2015 年	INAS
信息管理	Skills Framework for the Information Age，第 6 版，2015 年	IRMG

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
数据清理政策	概述管理层对数据清理做出的承诺。规定频率、准则和问责制；记录可用的方法、解决方案和工具。	CMMI 数据管理成熟度模型，2014 年	数据清理
数据管理政策	描述组织做出的在整个数据生命周期（从创建到交付、维护和归档）内管理数据资产的承诺。		
数据质量评估政策	描述组织的数据质量保证评估理念，以确保做出会影响组织的决策时所用数据的完整性。指明数据质量评估的频率、准则和问责制。概述可用的方法、解决方案和工具。	(1) CMMI 数据管理成熟度模型，2014 年；(2) 美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	(1) Data Quality Assessment；(2) 3.20 System and information integrity (SI-1)
隐私政策	记录个人数据的收集、使用、披露和管理。可用于识别个人身份的任何数据均为个人数据，包括但不限于姓名、地址、出生日期、婚姻状况、联系信息、身份证颁发日期和到期日期、财务记录、信用信息、病史、旅行目的地以及采购商品或服务的意图。隐私政策旨在说明企业会如何收集、存储和发布个人信息；客户何时和以何种方式获悉其特定信息已被收集，该等信息是否会予以保密、与合作伙伴分享或出售给其他公司或企业。该政策强制要求遵守关于数据保护的相关法律。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
营造为组织的数据资产共担责任的文化；确认数据资产的潜在价值，并确保数据资产治理和管理的角色及责任清晰明确。	CMMI 数据管理成熟度模型，2014 年	Data Governance
提高数据完整性、准确性、完全性和保护的相关意识，以建立数据质量文化。将数据质量与企业的核心价值相关联。持续传达数据丢失所产生的影响和风险。确保员工了解未遵守数据质量文化所造成的真实成本。	CMMI 数据管理成熟度模型，2014 年	数据质量

G. 组件：服务、基础设施和应用程序
• 数据建模工具 • 数据贮存库

4.3 内部构建、外部采购和实施 (BAI)

01 妥当管理的计划

02 妥当管理的需求定义

03 妥当管理的解决方案识别和构建

04 妥当管理的可用性和容量

05 妥当管理的组织变更

06 妥当管理的 IT 变更

07 妥当管理的 IT 变更接受和交接

08 妥当管理的知识

09 妥当管理的资产

10 妥当管理的配置

11 妥当管理的项目

领域：内部构建、外部采购和实施 管理目标：BAI01 — 妥当管理的计划	焦点领域：COBIT 核心模型

描述

根据标准计划管理方法管理投资组合中的所有计划，使其与企业战略保持一致，并以协调一致的方式进行。启动、规划、控制和执行计划，并监控计划的预期价值。

目的

实现期望的业务价值，降低因意外的延迟、成本和价值流失带来的风险。为此，应改进与业务部门和最终用户的沟通并提高他们的参与度，确保计划交付成果和计划内后续项目的价值和质量，并最大程度地提高对投资组合的贡献。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	• AG03 通过 I&T 促成的投资和服务组合所实现的效益 • AG09 在预算内按时交付计划且满足要求和质量标准

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG03	a. 达到或超过业务案例宣称效益的 I&T 促成的投资的百分比 b. 实现预期效益（如服务水平协议所述）的 I&T 服务的百分比
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度	AG09	a. 在预算内按时交付的计划/项目的数量 b. 因质量缺陷需要重大返工的计划的数量 c. 对计划/项目质量满意的利益相关方的百分比
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比		

A. 组件：流程

管理实践	指标示例
BAI01.01 维护计划管理的标准方法。 维护计划管理的标准方法，以便开展治理和管理审查、决策和交付管理活动。这些活动应始终关注业务价值和目标（即需求、风险、成本、日程表和质量目标）。	a. 根据既定的标准方法取得成功的计划百分比 b. 对计划管理满意的利益相关方的百分比

活动	能力级别
1. 维护和实施标准的计划管理方法，确保该方法与企业的特定环境保持一致，并运用基于既定流程和相应技术的良好实践。确保该方法涵盖整个生命周期和需要遵循的科目，包括范围、资源、风险、成本、质量、时间、沟通、利益相关方参与、采购、变更控制、整合和效益实现的管理。	2
2. 部署计划办公室或项目管理办公室 (PMO)，为整个组织的计划和项目管理维护标准方法。PMO 通过创建和维护必要的项目文档模板、为计划/项目经理提供培训和最佳实践，以及跟踪项目管理所用最佳实践的相关指标等方式，为所有计划和项目提供支持。在某些情况下，PMO 还会向高级管理层和/或利益相关方报告计划/项目进展情况，帮忙排定项目优先级，并确保所有项目都能支持企业的总体业务目标。	3
3. 根据计划管理方法的使用情况对汲取的经验教训进行评估，并对方法进行相应的更新。	4

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	
管理实践	**指标示例**
BAI01.02 启动计划。 启动计划，以确认实现预期效益并获得继续实施的授权。这包括在计划赞助方面达成共识、通过批准概念业务案例确认计划的授权、任命计划董事会或委员会成员、生成计划简介、审查和更新业务案例、制定效益实现计划，以及获得发起人的授权以继续执行。	a. 业务所有者提出的 I&T 举措/项目的百分比 b. 已分配责任的战略举措的百分比 c. 在业务案例未获批准的情况下开展的计划的百分比 d. 批准企业需求、范围、计划内成果和计划风险水平的利益相关方的百分比

活动	能力级别
1. 在计划支持方面达成共识。任命计划董事会/委员会成员，这些成员在计划中享有战略利益，负责做出投资决策，将会受到计划的重大影响，并且是实现变更交付的必要人员。	2
2. 为计划任命具备相应能力和技能的专职经理，以采用有效且高效的方式管理该计划。	
3. 与发起人和利益相关方确认计划的授权。阐明该计划的战略目标、潜在的交付战略、预期的改进和效益，以及该计划如何与其他举措保持一致。	3
4. 为计划制定详细的业务案例。确保所有关键利益相关方参与制定和记录过程，充分理解预期的企业成果、这些成果的衡量方式、所需举措的完整范围、涉及的风险以及对企业所有方面产生的影响。确定并评估备选行动方案，以实现预期的企业成果。	
5. 制定将在整个计划期间妥当管理的效益实现计划，确保计划内的效益始终具有责任人并且得到实现、维持和优化。	
6. 准备初始（概念）计划业务案例，提供关于目的、对业务目标的贡献、预期创造的价值、时间框架等方面的关键决策信息。提交案例以获得批准。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	
管理实践	**指标示例**
BAI01.03 管理利益相关方的参与。 管理利益相关方的参与，确保积极地与所有利益相关方交换准确、一致且及时的信息。这包括制定计划、识别利益相关方、推动他们参与并管理他们的期望。	a. 利益相关方对参与度的满意程度 b. 有效参与的利益相关方的百分比

活动	能力级别
1. 规划如何识别、分析、联系和管理项目生命周期内企业内外部的利益相关方。	3
2. 通过建立和维护相应级别的协调、沟通和联络来识别、联系和管理利益相关方，确保他们参与该计划。	
3. 分析利益相关方的利益和要求。	
4. 遵循合作协议中关于业务流程中的共享数据和数据使用的既定流程。	4

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 10. Project communications management
管理实践	**指标示例**
BAI01.04 制定和维护计划方案。 制定项目以便为其执行奠定初步基础。通过确定工作范围以及可达到目标和创造价值的可交付成果，确保项目成功执行。在项目的完整经济生命周期中维护和更新计划方案和业务案例，确保符合战略目标并反映现状和最新见解。	a. 不符合价值衡量标准的项目状态审查频率 b. 在缺少更新且有效的计划价值图的情况下实施的进行中计划的百分比

A. 组件：流程（续）	
活动	**能力级别**
1. 具体指明多个项目的资金、成本、日程安排和相互依存关系。	2
2. 定义和记录涵盖所有项目的计划方案。包括企业实现变更需要什么；计划的目的、使命、愿景、价值观、文化、产品和服务；业务流程；人员技能和数量；与利益相关方、客户、供应商和其他人的关系；技术需求；实现该计划的预期企业成果所需的组织结构调整。	3
3. 确保在所有项目和整个计划中有效地沟通计划方案和进度报告。确保对个别计划所做的任何变更都会反映到其他企业计划方案中。	
4. 维护计划方案以确保其保持最新状态，并且与当前战略目标、实际进展以及成果、效益、成本和风险方面的重大变化保持一致。让业务部门在整个过程中推进目标并确定工作优先级，确保设计的计划符合企业要求。审查单个项目的进展情况并根据需要调整项目，以满足计划的里程碑和版本发布。	
5. 在整个项目的经济生命周期中，更新和维护业务案例和效益登记表，以识别和确定因执行该计划所产生的关键效益。	
6. 指定计划预算以反映完整经济生命周期的成本以及相关的财务和非财务效益。	
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	
管理实践	**指标示例**
BAI01.05 启动和执行计划。 启动和执行计划，以获取和指导完成计划方案中定义的项目目标和效益所需的资源。根据阶段-关卡或版本审查标准准备阶段-关卡、迭代周期或版本审查，以报告进度并确保资金案例通过下一个阶段-关卡或版本审查。	a. 利益相关方签字批准活动计划的阶段-关卡审查的百分比 b. 对偏离计划的情况进行根本原因分析并实施必要补救措施的数量
活动	**能力级别**
1. 根据资金审查和各个阶段-关卡审查的批准情况，为实现计划成果所需的必要项目进行计划、资源安排和委任。	3
2. 采用一致的方式实现业务效益和目标，化解风险和满足利益相关方的需求，以此管理每个计划或项目，确保决策和交付活动专注于价值。	
3. 协定开发流程阶段（开发检查点）。每个阶段结束时，就经批准的衡量标准与利益相关方展开正式讨论。在顺利完成功能、性能和质量审查之后以及最终确定阶段活动之前，获得所有利益相关方和发起人/业务流程所有者的正式批准和签字。	
4. 在整个计划期间执行效益实现流程，确保计划内的效益始终具有责任人并且有可能实现、维持和优化。参照阶段-关卡或迭代周期和版本审查时的绩效目标，监控和报告效益的实现情况。对偏离计划的情况执行根本原因分析，确定并实施任何必要的补救措施。	4
5. 计划审计、质量审查、阶段/阶段-关卡审查和已实现效益的审查。	
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
BAI01.06 监控、控制和报告计划成果。 在投资的完整经济生命周期中参照计划来监控和控制绩效，包括计划层面的解决方案交付和企业层面的价值/成果。将绩效报告给计划指导委员会和发起人。	a. 已实现的预期计划效益的百分比 b. 已监控绩效并及时采取必要的补救措施的计划百分比

活动	能力级别
1. 更新运营 I&T 组合，以反映计划造成的相关 I&T 服务、资产或资源组合变化。	3
2. 监控和控制总体计划和计划内项目的绩效，包括业务和 IT 对项目的贡献。采用及时、完整且准确的方式进行报告。报告内容可能包括时间安排、资金、功能、用户满意度、内部控制和责任认可情况。	4
3. 参照企业和 I&T 战略及目标，监控和控制相关绩效。向管理层报告实施的企业变更、效益实现计划中的效益实现情况，以及效益实现流程的充分性。	
4. 监控和控制因计划而创建或变更的 IT 服务、资产和资源。注明实施日期和投入服务的日期。向管理层报告绩效水平、维持的服务交付和价值贡献。	
5. 参照关键衡量标准（如范围、进度、质量、效益实现、成本、风险、速度）管理计划绩效，识别偏离计划的情况并视需要及时采取补救措施。	
6. 监控单个项目在预期能力交付、进度、效益实现、成本、风险或其他指标方面的绩效。确定对计划绩效的潜在影响，并视需要及时采取补救措施。	
7. 根据阶段-关卡、版本或迭代周期审查标准执行审查，以报告计划进展，让管理层能够做出计划是否可行或是否需要调整的决策，以及批准下一个阶段-关卡、版本或迭代周期所需的资金。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
BAI01.07 管理计划质量。 制定和执行符合质量管理标准 (QMS) 的质量管理计划、流程和实践。描述计划质量和实施方法。应由所有相关方正式审批计划并达成共识，并将其纳入整合的项目群计划中。	a. 零错误地按包构建 (build-to-package) 的百分比 b. 每次关卡审查时获得批准的计划交付成果的百分比

活动	能力级别
1. 确定在项目规划期间为新系统或修改后的系统提供鉴证支持所需的鉴证任务和实践，并将其包含到整合计划中。确保这些任务提供证明内部控制和安全/隐私解决方案满足既定要求的鉴证。	3
2. 为计划交付成果提供质量保证，确定责任和职责、质量审查流程、成功标准和绩效指标。	
3. 定义对计划中的可交付成果质量进行独立验证和校验的任何要求。	4
4. 根据质量管理计划和质量管理体系 (QMS) 执行质量保证和控制活动。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
BAI01.08 管理计划风险。 通过系统性的流程（规划、识别、分析、应对和监控可能导致不希望的变更的领域或事件）消除或最大程度减少与计划相关的特定风险。定义并记录计划管理面临的任何风险。	a. 未进行适当风险评估的计划数量 b. 符合企业风险管理框架的计划的百分比

活动	能力级别
1. 制定符合企业风险管理 (ERM) 框架的正式风险管理方法。确保该方法包括风险识别、分析、应对、缓解、监控和控制。	3
2. 为具备相应技能的人员分配执行计划内的企业风险管理流程的职责，并确保将此纳入解决方案开发实践中。考虑将此角色分配给独立团队，尤其是在需要客观视点或该计划被视为关键计划时。	
3. 在整个计划中持续进行风险评估（识别和量化风险）。在计划治理结构内适当地管理和沟通风险。	
4. 确定规避、接受或缓解风险的行动的所有者。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
BAI01.09 关闭计划。 当确认已实现预期价值，或依据计划设定的价值标准明显无法实现预期价值时，则从有效投资组合中删除该计划。	a. 实现预期价值后成功关闭的计划的百分比 b. 从计划启动到检测到可实现价值之间的时间

活动	能力级别
1. 让计划有序关闭，包括正式批准、解散计划组织和支持职能、确认可交付成果和终止沟通。	3
2. 审查并记录汲取的经验教训。计划终止后，将其从有效投资组合中删除。将产生的任何能力转移到运营资产组合，以确保继续创造和维持该价值。	4
3. 落实责任和流程，确保企业继续优化服务、资产或资源的价值。未来某个时间可能需要进行额外投资，以确保实现上述目标。	5

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所，Framework for Improving Critical Infrastructure Cybersecurity，第 1.1 版，2018 年 4 月	RS.IM Improvements

B. 组件：组织结构												
关键管理实践	首席执行官	首席风险官	首席信息官	I&T 治理委员会	业务流程所有者	（计划/项目）指导委员会	计划经理	项目管理办公室	架构总监	开发总监	IT 运营总监
BAI01.01 维护计划管理的标准方法。	A		R	R			R				
BAI01.02 启动计划。		R			R	A	R	R			
BAI01.03 管理利益相关方的参与。					R	A	R	R			
BAI01.04 制定和维护计划方案。						A	R	R			
BAI01.05 启动和执行计划。			R		R	A	R	R			
BAI01.06 监控、控制和报告计划成果。			R			A	R	R	R	R	R
BAI01.07 管理计划质量。					R	A	R	R			
BAI01.08 管理计划风险。		R			R	A	R	R		R	
BAI01.09 关闭计划。			R		R	A	R	R		R	

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
BAI01.01 维护计划管理的标准方法。	自	描述	描述	至
	APO03.04	• 实施阶段描述 • 架构治理要求	更新后的计划管理方法	内部
	APO05.04	更新的计划、服务和资产组合		
	APO10.04	识别的供应商交付风险		
	EDM02.03	阶段-关卡审查的要求		
	EDM02.04	改进实现价值的措施		

C. 组件：信息流和信息项（另请参阅第 3.6 节）（续）				
管理实践	输入		输出	
	自	描述	描述	至
BAI01.02 启动计划。	APO03.04	• 资源要求 • 实施阶段描述	计划授权和概要	APO05.02
	APO05.02	计划业务案例	计划概念业务案例	APO05.02
	APO07.03	技能和能力矩阵	计划的效益实现规划	APO05.02；APO06.05
	BAI05.02	共同愿景和目标		
BAI01.03 管理利益相关方的参与。			利益相关方参与有效性评估的结果	内部
			利益相关方参与计划	内部
BAI01.04 制定和维护计划方案。	APO05.02	包含 ROI 里程碑的精选计划	计划预算和效益登记表	APO05.05；APO06.05
	APO07.03	技能和能力矩阵	资源要求和角色	APO07.05；APO07.06
	APO07.05	业务和 IT 人力资源清单	计划方案	内部
	BAI05.02	实施团队和角色		
	BAI05.03	愿景沟通计划		
	BAI05.04	已确定的速效方案		
	BAI07.03	已批准的验收测试计划		
	BAI07.05	经批准的验收和生产发布		
BAI01.05 启动和执行计划。	BAI05.03	愿景沟通	计划目标实现情况的监控结果	APO02.04
			效益实现情况的监控结果	APO05.05；APO06.05
			计划的审计计划	MEA04.02

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
BAI01.06 监控、控制和报告计划成果。	**自**	**描述**	**描述**	**至**
	APO05.01	投资回报预期	阶段-关卡审查结果	APO02.04；APO05.03；EDM02.02
	APO05.02	业务案例评估	计划绩效的审查结果	MEA01.03
	APO05.03	投资组合绩效报告		
	APO05.05	• 效益结果和相关沟通 • 用于改进效益实现的纠正措施		
	APO07.05	• 资源短缺分析 • 资源利用记录		
	BAI05.04	效益沟通		
	BAI06.03	变更请求状态报告		
	BAI07.05	验收结果评估		
	EDM02.04	组合和计划绩效的反馈		
BAI01.07 管理计划质量。	APO11.01	质量管理计划	质量管理计划	BAI02.04；BAI03.06；BAI07.01
	APO11.02	客户对质量管理的要求	可交付成果的独立验证要求	BAI07.03
BAI01.08 管理计划风险。	APO12.02	风险分析结果	计划风险登记表	内部
	BAI02.03	• 需求风险登记表 • 风险缓解措施	计划风险评估结果	内部
	在 COBIT 外部	企业风险管理 (ERM) 框架	计划的风险管理计划	内部
BAI01.09 关闭计划。	BAI07.08	• 实施后审查报告 • 补救行动计划	计划终止和持续责任的沟通	APO05.04；APO07.06

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 4. Project integration management: Inputs and Outputs; Part 1: 6. Project schedule management: Inputs and Outputs; Part 1: 10. Project communications management: Inputs and Outputs; Part 1: 11. Project risk management: Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
Benefits management	Skills Framework for the Information Age，第 6 版，2015 年	BENM
业务计划制定	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	A. Plan—A.3. Business Plan Development
计划管理	Skills Framework for the Information Age，第 6 版，2015 年	PGMG
项目和组合管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage—E.2. Project and Portfolio Management

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
计划/项目管理政策	指导与计划和项目有关的风险管理。详细说明关于计划和项目管理的管理职位和期望。在计划/项目执行期间处理有关绩效、预算、风险分析、不良事件的报告和缓解的问责、目的和目标。	PMBOK Guide，第 6 版，2017 年	Part 1: 2.3.1 Processes, policies and procedures

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
确保组织理解并支持企业范围的计划管理的价值。在考虑组织结构和业务环境的前提下，在整个企业范围内建立支持持续实施计划管理的文化。确保计划办公室能够统揽企业组合中的所有计划。		

G. 组件：服务、基础设施和应用程序
计划管理工具

领域：内部构建、外部采购和实施 管理目标：BAI02 — 妥当管理的需求定义	焦点领域：COBIT 核心模型

描述

在外部采购或创建之前确定解决方案并分析要求，确保其符合企业在业务流程、应用、信息/数据、基础设施和服务方面的战略要求。与受影响的利益相关方协调，审查可行的备选方案，包括相对成本和效益、风险分析，以及批准要求和建议的解决方案。

目的

创建最优解决方案，在满足企业需求的同时最大程度降低风险。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	• AG05 提供符合业务需求的 I&T 服务 • AG06 将业务需求转化为可运作的解决方案的敏捷性 • AG09 在预算内按时交付计划且满足要求和质量标准

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG05	a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度	AG06	a. 业务高管对 I&T 响应新需求的满意度水平 b. 新的 I&T 相关服务和应用程序的平均上市时间 c. 将战略 I&T 目标转化为议定的已批准举措所需的平均时间 d. 受最新基础设施和应用支持的关键业务流程的数量
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比	AG09	a. 在预算内按时交付的计划/项目的数量 b. 因质量缺陷需要重大返工的计划的数量 c. 对计划/项目质量满意的利益相关方的百分比

A. 组件：流程	
管理实践	**指标示例**
BAI02.01 定义和维护业务职能和技术要求。 基于业务案例，识别和指明业务信息、职能、技术和控制要求，确定优先级并达成一致意见，以涵盖实现所建议的 I&T 促成的业务解决方案预期成果所需的全部举措的范围/理解。	a. 由于不符合企业需求和期望而重新制定的要求的百分比 b. 通过同行评审、模型验证或操作原型等方法进行验证的要求的百分比

活动	能力级别
1. 确保以所有利益相关方都能理解的方式考虑、捕获和记录利益相关方的所有要求（包括相关的验收标准）并排定优先级，同时意识到这些要求在实施过程中可能发生变化和进一步细化。	2
2. 围绕如何弥补当前业务能力与目标业务能力需求之间的差距以及用户（员工、客户等）如何与解决方案交互和使用解决方案来阐述业务需求。	
3. 基于用户体验设计和经确认的利益相关方要求，具体说明信息、功能和技术要求并确定其优先级。	
4. 确保要求符合企业政策和标准、企业架构、战略性和策略性 I&T 计划、内部和外包业务及 IT 流程、安全要求、监管要求、人员能力、组织结构、业务案例和支持技术。	3
5. 将信息控制要求纳入业务流程、自动化流程和 I&T 环境，以化解信息风险并遵守法律、法规和商业合同。	
6. 确认接受这些要求的关键方面，包括企业规则、用户体验、信息控制、业务连续性、法律和监管合规性、可审计性、人体工程学、可操作性和可用性、安全性、机密性和支持文件。	
7. 随着对解决方案的理解逐渐深入，跟踪和控制解决方案在整个生命周期内的范围、要求和变化。	
8. 定义并实施与企业考虑实施的举措的规模、复杂性、目标和风险相称的需求定义和维护程序以及需求贮存库。	
9. 通过同行评审、模型验证或操作原型等方法验证所有要求。	

相关指南（标准、框架、合规性要求）	详细参考
ISF, The Standard of Good Practice for Information Security 2016	SD2.1 Specifications of Requirements
ISO/IEC 27002:2013/Cor.2:2015(E)	14.1 Security requirements of information systems
ITIL 第 3 版，2011 年	Service Design, 5.1 Requirements engineering
PMBOK Guide，第 6 版，2017 年	Part 1: 5. Project scope management

管理实践	指标示例
BAI02.02 执行可行性分析并制定备选解决方案。 对潜在的备选解决方案执行可行性分析，评估其可用性并选择首选方案。如果恰当，实施所选的方案作为试点，以确定可能的改进。	a. 建议的解决方案实现业务案例目标的百分比 b. 建议的解决方案满足要求的百分比

活动	能力级别
1. 根据企业架构确定采购或开发解决方案所需的行动。充分考虑范围和/或时间和/或预算限制。	2
2. 与所有利益相关方一起审查备选解决方案。根据可行性标准（包括风险和成本）选择最合适的方案。	
3. 将首选行动方案转化为高层采购/开发计划，确定将要使用的资源和需要做出可行/不可行决策的阶段。	3
4. 定义并执行可行性分析、试点或基本工作解决方案，简明扼要地描述备选解决方案，并衡量这些解决方案如何满足业务和功能要求。还应包括相应的技术和经济可行性评估。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
BAI02.03 管理需求风险。 识别和记录与企业要求、假设和建议的解决方案相关的功能、技术和信息处理相关风险，排定优先级并加以缓解。	a. 相应的风险响应未涵盖需求风险的百分比 b. 记录的需求风险的详细程度 c. 预计发生所列需求风险的概率和影响以及风险响应的完整性

活动	能力级别
1. 识别质量、功能和技术需求风险（例如，由于缺乏用户参与、不切实际的期望、开发人员添加不必要的功能、不切实际的假设等引起的风险）。	3
2. 确定对需求风险的相应风险响应。	
3. 通过估计发生概率以及对预算和进度的影响来分析已识别的风险。评估相应风险响应行动的预算影响。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
BAI02.04 获取对需求和解决方案的批准。 协调来自受影响的利益相关方的反馈。在预定的关键阶段，就功能和技术要求、可行性分析、风险分析和建议的解决方案获得业务发起人或产品所有者的批准和签字认可。	a. 利益相关方对要求的满意度水平 b. 在阶段审查期间发现设计异常的解决方案的数量 c. 利益相关方未批准业务案例相关解决方案的百分比

活动	能力级别
1. 确保业务发起人或产品所有者根据业务案例最终选定解决方案、采购方法和高层次设计。获取受影响的利益相关方（如业务流程所有者、企业架构师、运营经理、安全人员、隐私官）的必要批准。	3
2. 在每个关键项目阶段、迭代周期或版本的全过程和结束时获得质量审查。参照原始验收标准对结果进行评估。让业务发起人和其他利益相关方签字批准每次成功完成的质量审查。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构														
关键管理实践	**首席风险官**	**首席信息官**	**业务流程所有者**	**（计划/项目）指导委员会**	**计划经理**	**项目经理**	**项目管理办公室**	**关系经理**	**架构总监**	**开发总监**	**IT 运营总监**	**信息安全经理**	**隐私官**
BAI02.01 定义和维护业务职能和技术要求。			R	A	R	R	R	R	R	R		R	R
BAI02.02 执行可行性分析并制定备选解决方案。			R	A	R	R	R			R			
BAI02.03 管理需求风险。	R	R	R	A	R	R	R			R	R	R	R
BAI02.04 获取对需求和解决方案的批准。			R	A	R	R	R					R	R

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
BAI02.01 定义和维护业务职能和技术要求。	APO01.07	• 数据分类准则 • 数据安全和控制准则 • 数据完整性程序	需求定义贮存库	BAI03.01； BAI03.02； BAI03.12； BAI04.01； BAI05.01
	APO03.01	架构原则	已确认的利益相关方验收标准	BAI03.01； BAI03.02； BAI03.12； BAI04.03； BAI05.01； BAI05.02
	APO03.02	• 基准指标领域说明和架构定义 • 信息架构模型	需求变更请求记录	BAI03.09
	APO03.05	解决方案开发指导		
	APO10.02	供应商信息请求 (RFI) 和需求建议书 (RFP)		
	APO11.02	验收标准		
	APO14.02	业务词汇表		
BAI02.02 执行可行性分析并制定备选解决方案。	APO03.05	解决方案开发指导	高层采购/开发计划	APO10.02； BAI03.01
	APO10.01	供应商目录	可行性分析报告	BAI03.02； BAI03.03； BAI03.12
	APO10.02	• 供应商信息请求 (RFI) 和需求建议书 (RFP) • RFI 和 RFP 评估 • 供应商评估的决策结果		
	APO11.02	验收标准		
BAI02.03 管理需求风险。			需求风险登记表	BAI01.08； BAI03.02； BAI04.01； BAI05.01； BAI11.06
			风险缓解措施	BAI01.08； BAI03.02； BAI05.01
BAI02.04 获取对需求和解决方案的批准。	BAI01.07	质量管理计划	已批准的质量审查	APO11.03
	BAI11.05	项目质量管理计划	发起人批准需求和建议的解决方案	BAI03.02； BAI03.03； BAI03.04

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 5. Project management scope: Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
应用程序设计	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	A. Plan—A.6. Application Design
业务分析	Skills Framework for the Information Age，第 6 版，2015 年	BUAN
业务流程改进	Skills Framework for the Information Age，第 6 版，2015 年	BPRE
需求识别	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	D. Enable—D.11. Needs Identification
需求定义和管理	Skills Framework for the Information Age，第 6 版，2015 年	REQM
用户体验分析	Skills Framework for the Information Age，第 6 版，2015 年	UNAN

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
软件开发政策	通过列出需要遵循的所有协议和标准，使整个组织的软件开发实现标准化。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
建立确保采用一致、可靠的流程定义需求的文化。确保流程在开发需求与企业战略需求之间保持明确的一致性。		

G. 组件：服务、基础设施和应用程序
需求定义和文档工具

领域：内部构建、外部采购和实施 管理目标：BAI03 — 妥当管理的解决方案识别和构建	焦点领域：COBIT 核心模型

描述

根据企业在设计、开发、采购以及与供应商的合作等方面的要求，建立和维护确认的产品和服务（技术、业务流程和工作流程）。管理业务流程、应用、信息/数据、基础设施和服务的配置、测试准备、测试、需求管理和维护。

目的

确保以敏捷和可扩展的方式交付数字产品和服务。建立及时、合算的并且能够支持企业战略和运营目标的解决方案（技术、业务流程和工作流程）。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标		一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	→	• AG05 提供符合业务需求的 I&T 服务 • AG06 将业务需求转化为可运作的解决方案的敏捷性 • AG09 在预算内按时交付计划且满足要求和质量标准
企业目标的指标示例		**一致性目标的指标示例**
EG01 a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间		AG05 a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG08 a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		AG06 a. 业务高管对 I&T 响应新需求的满意度水平 b. 新的 I&T 相关服务和应用程序的平均上市时间 c. 将战略 I&T 目标转化为议定的已批准举措所需的平均时间 d. 受最新基础设施和应用支持的关键业务流程的数量
EG12 a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比		AG09 a. 在预算内按时交付的计划/项目的数量 b. 因质量缺陷需要重大返工的计划的数量 c. 对计划/项目质量满意的利益相关方的百分比

A. 组件：流程

管理实践	指标示例
BAI03.01 设计高层级解决方案。 为技术、业务流程和工作流程方面的解决方案开发和记录高层设计。使用达成共识并适当分阶段或快速敏捷的开发方法。确保符合 I&T 战略和企业架构。在详细设计期间或构建阶段发生重大问题时，或者随着解决方法的发展演变，重新评估和更新设计。采用以用户为中心的方法；确保利益相关方积极参与设计并批准每个版本。	a. 审查设计时发现缺陷的数量 b. 利益相关方参与设计并批准每个版本的百分比

A. 组件：流程（续）	
活动	**能力级别**
1. 制定高层设计规范，用于将建议的解决方案转化为能够满足业务和企业架构要求的业务流程、支持服务、工作流程、应用程序、基础设施及信息贮存库之高层设计。	2
2. 让拥有合适资质和经验的用户体验设计人员和 IT 专家参与到设计过程中，确保设计提供的解决方案能够以最优方式使用建议的 I&T 能力来完善业务流程。	
3. 创建一个符合组织设计标准的设计。确保该设计的详细程度适用于相应解决方案和开发方法，并且与业务、企业及 I&T 战略、企业架构、安全/隐私计划以及适用法律、法规和合同保持一致。	
4. 在获得质量保证批准之后，将最终的高层设计提交给项目利益相关方和发起人/业务流程所有者，由其根据议定的标准进行审批。该设计将在整个项目过程中随着理解的加深不断完善。	
相关指南（标准、框架、合规性要求）	**详细参考**
ISF, The Standard of Good Practice for Information Security 2016	SD2.2 System Design
管理实践	**指标示例**
BAI03.02 设计详细的解决方案组件。 逐步开发、记录和细化详细设计。使用达成共识的适当分阶段或快速敏捷的开发方法，处理所有组件（业务流程及相关的自动化和手动控制，支持 I&T 应用程序、基础设施服务和技术产品，以及合作伙伴/供应商）。确保详细设计包含内外部服务水平协议 (SLA) 和运营水平协议 (OLA)。	a. 审查设计时发现缺陷的数量 b. 进行中的设计变更的数量
活动	**能力级别**
1. 逐步设计需要与新应用程序系统一起执行的业务流程活动和工作流程，以满足企业目标，包括设计人工控制活动。	2
2. 设计应用程序处理步骤。这些步骤包括指定交易类型及业务处理规则、自动化控制、数据定义/业务目标、用例、外部接口、设计限制和其他要求（例如，许可、法律、标准和国际化/本地化）。	
3. 根据企业架构标准对数据输入和输出进行分类。指定源数据集合设计。记录交易处理的数据输入（任何来源）和验证以及验证方法。设计既定的输出，包括数据源。	
4. 设计系统/解决方案接口，包括任何自动数据交换。	
5. 设计数据存储、位置、检索和可恢复性。	
6. 设计适当的冗余、恢复和备份机制。	
7. 设计用户与系统应用程序之间的接口，使其易于使用和自编文档。	3
8. 考虑解决方案的基础设施性能需求带来的影响，留意计算资产的数量、带宽强度和信息的时间敏感性。	
9. 在整个生命周期中，主动评估设计缺陷（例如，不一致、不清晰、潜在缺陷）。需要时确定改进方面。	
10. 提供审计交易和识别处理错误的根本原因的能力。	
相关指南（标准、框架、合规性要求）	**详细参考**
ISF, The Standard of Good Practice for Information Security 2016	SD2.2 System Design

A. 组件：流程（续）	
管理实践	**指标示例**
BAI03.03 开发解决方案组成部分。 按照详细设计，根据开发、记录、质量保证 (QA) 及审批方面的标准与要求，在独立的环境中逐步开发解决方案组件。确保涉及了业务流程、提供支持的 I&T 应用程序和基础设施服务、服务和技术产品以及合作伙伴/供应商服务方面的所有控制要求。	a. 阶段审查期间在解决方案中发现的设计异常的数量 b. 业务流程、支持服务、应用程序及基础设施和信息贮存库的详细设计数量

活动	能力级别
1. 在独立的环境中，为业务流程、支持服务、应用程序、基础设施和信息贮存库开发建议的详细设计。	2
2. 当第三方提供商参与解决方案开发时，确保在合同义务中规定和遵守维护、支持、开发标准和许可事宜。	
3. 跟踪变更请求以及设计、性能和质量审查。确保所有受影响的利益相关方积极参与。	
4. 根据规定的标准记录所有解决方案组件。对所有已开发的组件和相关文档进行版本控制。	
5. 评估解决方案的定制和配置对采购解决方案的性能与效率的影响，以及对解决方案与现有应用程序、操作系统和其他基础设施之间协同的影响。根据需要调整业务流程以便利用应用程序能力。	3
6. 确保使用既定的高安全性或限制访问的基础设施组件的责任，并确保基础设施组件的开发和集成人员了解这些责任。应对它们的使用进行监控和评估。	

相关指南（标准、框架、合规性要求）	详细参考
ISF, The Standard of Good Practice for Information Security 2016	SD1.2 System Development Environments
ISO/IEC 27002:2013/Cor.2:2015(E)	14.2 Security in development and support processes
ITIL 第 3 版，2011 年	Service Strategy, 5.5 IT service strategy and application development
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.18 System and services acquisition (SA-3)

管理实践	指标示例
BAI03.04 采购解决方案组成部分。 基于收购计划，秉承需求和详细设计、架构原则和标准、企业的整体采购与合同程序、QA 需要和审批标准，采购解决方案组成部分。确保供应商确认并遵守所有法律及合同要求。	a. 获得认证的供应商的百分比 b. 参与协作设计的供应商的百分比

活动	能力级别
1. 制定并维护解决方案组件采购计划。考虑项目生命周期中将来的扩容性、迁移成本、风险和升级的灵活性。	3
2. 审查和批准所有采购计划。考虑风险、成本、效益以及与企业架构标准的技术一致性。	
3. 评估和记录为适用已购解决方案而对业务流程调整的程度。	
4. 在采购流程中的关键决策点进行必要的审批。	
5. 在资产清单中存档所有基础设施和软件采购的接收确认。	

相关指南（标准、框架、合规性要求）	详细参考
ISF, The Standard of Good Practice for Information Security 2016	SD2.3 Software Acquisition
美国国家标准与技术研究所，Framework for Improving Critical Infrastructure Cybersecurity，第 1.1 版，2018 年 4 月	3.4 Buying Decisions
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.18 System and services acquisition (SA-4)

A. 组件：流程（续）	
管理实践	**指标示例**
BAI03.05 构建解决方案。 安装和配置解决方案，并与业务流程活动集成。在配置和集成硬件与基础设施软件期间，实施控制、安全、隐私和可审计性措施来保护资源，确保可用性和数据完整性。根据新解决方案更新产品或服务目录。	a. 预估的与最终的开发工作量之间的差距 b. 报告的软件问题数量 c. 审查错误的数量

活动	能力级别
1. 根据详细的规范和质量要求，集成和配置业务及 IT 解决方案组件与信息贮存库。在业务流程配置中考虑用户、业务利益相关方和流程所有者的角色。	2
2. 必要时，完成和更新业务流程和操作手册，来阐述相关实施所特有的任何定制或特殊情况。	
3. 在解决方案组件的集成和配置过程中，考虑所有相关的信息控制要求。在适当情况下，将业务控制的实施纳入到自动化应用程序控制中，使处理过程精确、完整、及时、获得授权且可审计。	
4. 在配置和集成硬件与基础设施软件期间实施审计轨迹，以保护资源并确保可用性和完整性。	3
5. 考虑定制和配置的累加效应（包括未遵循正式设计规范的微小变更）何时要求对解决方案和相关功能进行高级再评。	
6. 配置已购应用程序软件以满足业务需求。	
7. 根据业务需求，为相关的内外部目标群体定义产品和服务目录。	
8. 确保解决方案组件与配套测试的协同，最好是自动化的。	

相关指南（标准、框架、合规性要求）	详细参考
HITRUST CSF，第 9 版，2017 年 9 月	10.05 Security in Development & Support Processes
ISF, The Standard of Good Practice for Information Security 2016	SD2.4 System Build

管理实践	指标示例
BAI03.06 执行质量保证 (QA)。 制定符合 QMS 的 QA 计划、提供资源并执行 QA 计划，以达到需求定义以及企业的质量政策和程序中规定的质量。	a. 由于与需求不一致而返工的解决方案设计的数量 b. 记录的已执行监控活动的数量和稳健性

活动	能力级别
1. 制定 QA 计划和实践，例如，包括指定质量标准、验证和校验流程，定义如何审查质量，质量审查人员的必备资格，以及实现质量要求的角色和职责等。	3
2. 根据项目要求、企业政策、是否遵守开发方法、质量管理程序和验收标准，经常性地监控解决方案质量。	4
3. 适当地采用代码检查、测试驱动的开发实践、自动化测试、连续集成、穿行测试和应用程序测试。向应用程序软件开发团队和 IT 管理层报告监控和测试的结果。	
4. 监控所有质量异常情况，并实施任何纠正措施。维护所有审查、结果、异常和纠正的记录。在适当情况下，根据返工量和纠正措施，重新进行质量审查。	

相关指南（标准、框架、合规性要求）	详细参考
ISF, The Standard of Good Practice for Information Security 2016	SD1.3 Quality Assurance

A. 组件：流程（续）	
管理实践	**指标示例**
BAI03.07 准备解决方案测试。 构建测试计划和必要的环境，以测试独立和集成的解决方案组件。包括业务流程与支持服务、应用程序和基础设施。	a. 参与创建测试计划的业务用户的数量 b. 为测试创建的用例的数量和稳健性

活动	能力级别
1. 创建与企业环境和战略技术计划相适应的集成测试计划和实践。确保集成的测试计划和实践能够支持创建合适的测试及模拟环境，以帮助验证解决方案是否可在实际环境中成功运行并交付预期结果，以及控制是否充分。	2
2. 创建为解决方案提供全方位支持的测试环境。确保测试环境尽可能地反映真实状况，包括业务流程及程序、用户范围、交易类型和部署条件。	
3. 创建与计划和实践一致的测试程序，并允许评估解决方案在真实状况中的运行情况。确保测试程序根据用于定义角色、职责和测试标准的企业级标准来评估控制的充分性，并获得项目利益相关方和发起人/业务流程所有者的批准。	3
4. 记录并保存测试程序、用例、控制和参数，以便将来对应用程序进行测试。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	AD.DE Safeguard Development Environment
美国国家标准与技术研究所特别出版物 800-53， 修订版 5（草稿），2017 年 8 月	3.10 Maintenance (MA-2, MA-3)

管理实践	指标示例
BAI03.08 执行解决方案测试。 在开发期间，根据定义的测试计划和开发实践，在适当的环境中持续进行测试（包括控制测试）。让业务流程所有者和最终用户加入到测试团队中。识别和记录在测试期间发现的错误和问题，并确定其优先级。	a. 测试期间发现的错误数量 b. 完成测试所需的时间和工作量

活动	能力级别
1. 根据测试计划对解决方案及其组件进行测试。让团队外测试人员和有代表性的业务流程所有者及最终用户参与其中。确保测试只在开发和测试环境中进行。	2
2. 使用测试计划中明确定义的测试说明。考虑在自动化脚本测试和交互式用户测试之间取得适当平衡。	
3. 根据测试计划和实践进行所有测试。包括业务流程与 IT 解决方案组件的集成，以及非职能性需求（例如安全、隐私、协同和易用性）的集成。	
4. 识别和记录测试期间出现的错误并进行分类（如次要、重要和关键任务错误）。重复测试，直到解决所有重大错误为止。确保维护测试结果的审计轨迹。	
5. 根据测试计划记录测试结果，并向利益相关方传达测试结果。	

相关指南（标准、框架、合规性要求）	
CMMI Cybermaturity Platform，2018 年	AD.ST Secure Development Testing
ISF, The Standard of Good Practice for Information Security 2016	SD2.5 System Testing; SD2.6 Security Testing
美国国家标准与技术研究所特别出版物 800-53， 修订版 5（草稿），2017 年 8 月	3.18 System and services acquisition (SA-11)

A. 组件：流程（续）		
管理实践	**指标示例**	
BAI03.09 管理对需求的变更。 在整个项目生命周期内跟踪单个需求（包括所有被拒需求）的状态。管理对需求变更的审批。	a. 已跟踪且获批准的变更产生新错误的数量 b. 对变更管理流程满意的利益相关方的百分比	
活动		**能力级别**
1. 评估所有解决方案变更请求对解决方案开发、原始业务案例和预算的影响。对它们进行相应的分类并排定优先级。		3
2. 跟踪需求变更，使所有利益相关方能够监控、审查和审批变更。确保变更流程的结果得到所有利益相关方和发起人/业务流程所有者的充分理解和认同。		
3. 应用变更请求，保持解决方案组件的集成和配置的完整性。根据相关风险分析的结果（如对现有系统和流程或安全/隐私的影响）、成本效益平衡和其他要求，评估任何重大解决方案升级的影响，并按照议定的客观标准（如企业要求）对其进行分类。		
相关指南（标准、框架、合规性要求）	**详细参考**	
ISF, The Standard of Good Practice for Information Security 2016	SD2.9 Post-implementation Review	
管理实践	**指标示例**	
BAI03.10 维护解决方案。 制定并执行解决方案和基础设施组件的维护计划。包括对照业务需求和运营要求进行定期审查。	a. 维护需求未满意的数量 b. 维护需求满意和不满意的时间	
活动		**能力级别**
1. 制定并执行解决方案组件的维护计划。包括对照业务需求和运营要求定期进行审查，例如补丁管理、升级策略、风险、隐私、漏洞评估和安全要求等。		2
2. 评估建议的维护活动对当前解决方案设计、功能和/或业务流程的重要程度。考虑风险、用户影响和资源可用性。确保业务流程所有者了解指定变更维护的影响。		3
3. 如果对现有解决方案进行的重大变更导致当前设计和/或功能和/或业务流程发生重大改变，则应遵循适用于新系统的开发流程。要进行维护更新，则使用变更管理流程。		
4. 确保定期分析维护活动的模式和数量，以发现表明存在底层质量或性能问题的异常趋势，获取重大升级的成本/效益，或确定是否以更换替代维护。		4
相关指南（标准、框架、合规性要求）	**详细参考**	
ISO/IEC 27002:2013/Cor.2:2015(E)	14.3 Test data	
管理实践	**指标示例**	
BAI03.11 定义 IT 产品和服务并维护服务组合。 定义并确定新的或变更的 IT 产品或服务和服务水平选项。记录新的或变更的产品和服务定义及服务水平选项，以便更新到产品和服务组合中。	a. 签字批准新 I&T 服务的利益相关方的百分比 b. 在服务组合中记录的新的或变更的服务定义和服务水平选项的百分比。 c. 在服务组合中更新的新的或变更的服务定义和服务水平选项的百分比	

A. 组件：流程（续）	
活动	**能力级别**
1. 建议新的或变更的 IT 产品和服务的定义，确保其符合产品和服务的目的。将建议的定义记录在将要开发的产品和服务组合列表中。	3
2. 建议新的或变更的服务水平选项（服务时间、用户满意度、可用性、性能、容量、安全、隐私、连续性、合规性和易用性），以确保 IT 产品和服务适用。将建议的服务选项记录在组合中。	
3. 与业务关系管理人员和组合管理人员一起，就建议的产品和服务定义以及服务水平选项达成一致。	
4. 如果产品或服务变更在议定的审批权限范围内，则建立新的或变更的 IT 产品和服务或服务水平选项。否则，将变更转给组合管理人员进行投资审查。	
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	
管理实践	**指标示例**
BAI03.12 基于定义的开发方法设计方案。 按照总体战略和要求，使用适当的开发方法（即瀑布式、敏捷式或双模式 I&T 方法）设计、开发和实施解决方案。	a. 应用所选开发方法的解决方案开发项目的百分比 b. 根据所选战略调整的流程的百分比
活动	**能力级别**
1. 分析和评估不同开发方法（即瀑布式、敏捷式、双模式）对可用资源、架构要求、配置设置和系统刚性产生的影响。	3
2. 确定能够有效且高效地交付建议的解决方案，并且能够满足业务、架构和系统要求的适当开发方法和组织方法。根据需要，按照所选的战略调整流程。	
3. 根据所选开发方法的规定组建所需的项目团队。提供充分的培训。	
4. 如果需要，可以考虑应用双体系，即，让跨职能团队（数字工厂）使用与公司其他部门不同的技术、操作或管理方法，专注于开发一种产品或流程。将这些团队融入业务部门中，有利于传播新的敏捷开发文化，促使这种数字工厂方法成为规范。	
相关指南（标准、框架、合规性要求）	**详细参考**
ISF, The Standard of Good Practice for Information Security 2016	SD1.1 System Development Methodology

B. 组件：组织结构																				
关键管理实践	首席信息官	首席技术官	首席数字官	业务流程所有者	组合经理	（计划/项目）指导委员会	计划经理	项目经理	项目管理办公室	关系经理	架构总监	开发总监	IT 运营总监	IT 行政总监	服务经理	信息安全经理	业务连续性经理	隐私官
BAI03.01 设计高层级解决方案。		R		R		A	R	R	R	R		R				R		
BAI03.02 设计详细的解决方案组件。		R		R		A	R	R	R			R						
BAI03.03 开发解决方案组成部分。		R		R		A	R	R	R			R						
BAI03.04 采购解决方案组成部分。		R		R		A						R	R	R				
BAI03.05 构建解决方案。		R		R		A	R	R	R			R				R		
BAI03.06 执行质量保证 (QA)。		R		R		A	R	R	R			R						
BAI03.07 准备解决方案测试。		R		R		A						R	R		R	R	R	R
BAI03.08 执行解决方案测试。		R		R		A						R	R			R		R
BAI03.09 管理对需求的变更。		R		R		A	R	R	R		R	R				R		R
BAI03.10 维护解决方案。	A	R		R			R	R	R			R				R		R
BAI03.11 定义 IT 产品和服务并维护服务组合。	A														R	R		R
BAI03.12 基于定义的开发方法设计方案。	A		R		R		R	R										

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
BAI03.01 设计高层级解决方案。	APO03.01	架构原则	已批准的高层设计规范	BAI04.03; BAI05.01
	APO03.02	基准指标领域说明和架构定义		
	APO04.03	创新可能性的研究分析		
	APO04.04	创新想法的评估		
	BAI02.01	• 需求定义贮存库 • 利益相关方已确认的验收标准		
	BAI02.02	高层采购/开发计划		
BAI03.02 设计详细的解决方案组件。	APO03.01	架构原则	内部和外部 SLA	BAI04.02
	APO03.02	• 基准指标领域说明和架构定义 • 信息架构模型	已批准的详细设计规范	BAI04.03; BAI05.01
	APO03.05	解决方案开发指南		
	APO04.06	创新方法的评估		
	BAI02.01	• 需求定义贮存库 • 利益相关方已确认的验收标准		
	BAI02.02	可行性分析报告		
	BAI02.03	• 需求风险登记表 • 风险缓解措施		
	BAI02.04	由发起人批准需求和建议的解决方案		
BAI03.03 开发解决方案组成部分。	BAI02.02	可行性分析报告	记录的解决方案组件	BAI04.03; BAI05.05; BAI08.02; BAI08.03
	BAI02.04	由发起人批准需求和建议的解决方案		

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
	自	**描述**	**描述**	**至**
BAI03.04 采购解决方案组成部分。	BAI02.04	由发起人批准需求和建议的解决方案	已批准的采购计划	APO10.03
			资产清单的更新	BAI09.01
BAI03.05 构建解决方案。			已集成和配置的解决方案组件	BAI06.01
BAI03.06 执行质量保证 (QA)。	APO11.01	QMS 有效性审查的结果	质量审查结果、异常和纠正措施	APO11.04
	BAI01.07	质量管理计划	质量保证计划	APO11.04
	BAI11.05	项目质量管理计划		
BAI03.07 准备解决方案测试。			测试程序	BAI07.03
			测试计划	BAI07.03
BAI03.08 执行解决方案测试。	APO04.05	被拒绝举措的分析	测试结果沟通	BAI07.03
			测试结果日志和审计轨迹	BAI07.03
BAI03.09 管理对需求的变更。	APO04.05	概念验证举措的结果和建议	所有已批准和应用的变更请求的记录	BAI06.03
	BAI02.01	需求变更请求的记录		
BAI03.10 维护解决方案。			维护计划	APO08.05
			更新的解决方案组件和相关的文档	BAI05.05
BAI03.11 定义 IT 产品和服务并维护服务组合。	APO02.04	• 与目标能力的差距和实现目标能力所需的变更 • 目标环境的价值效益说明	更新的服务组合	APO05.04
	APO06.02	预算分配	服务定义	EDM02.01；DSS01.03
	APO06.03	• I&T 预算 • 预算沟通		
	APO08.05	潜在改进项目的定义		
	BAI10.02	配置基准指标		
	BAI10.03	已批准的基准指标变更		
	BAI10.04	配置状态报告		
	EDM04.01	资源和能力分配的指导原则		

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
BAI03.12 基于定义的开发方法设计解决方案。	**自**	**描述**	**描述**	**至**
	APO03.02	基准指标领域说明和架构定义		
	APO03.05	解决方案开发指南		
	APO07.03	技能和能力矩阵		
	BAI02.01	• 利益相关方已确认的验收标准 • 需求定义贮存库		
	BAI02.02	可行性分析报告		
	BAI10.02	配置基准指标		
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
应用程序开发	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	B. Build—B.1. Application Development
业务流程测试	Skills Framework for the Information Age，第 6 版，2015 年	BPTS
组件集成	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	B. Build—B.2. Component Integration
数据库设计	Skills Framework for the Information Age，第 6 版，2015 年	DBDS
文档制作	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	B. Build—B.5. Documentation Production
硬件设计	Skills Framework for the Information Age，第 6 版，2015 年	HWDE
端口/软件配置	Skills Framework for the Information Age，第 6 版，2015 年	PORT
编程/软件开发	Skills Framework for the Information Age，第 6 版，2015 年	PROG
发布和部署	Skills Framework for the Information Age，第 6 版，2015 年	RELM
解决方案架构	Skills Framework for the Information Age，第 6 版，2015 年	ARCH
解决方案部署	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	B. Build—B.4. Solution Deployment
系统设计	Skills Framework for the Information Age，第 6 版，2015 年	DESN
系统开发管理	Skills Framework for the Information Age，第 6 版，2015 年	DLMG
系统工程	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	B. Build—B.6. Systems Engineering

D. 组件：人员、技能和胜任能力（续）		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
系统安装/弃用	Skills Framework for the Information Age，第 6 版，2015 年	HSIN
系统集成	Skills Framework for the Information Age，第 6 版，2015 年	SINT
测试	Skills Framework for the Information Age，第 6 版，2015 年	TEST
测试	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	B. Build—B.3. Testing
用户体验设计	Skills Framework for the Information Age，第 6 版，2015 年	HCEV

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
维护政策	定义适当的软件和硬件组件支持，以确保更长的资产寿命，提高员工工作效率，维护可接受的用户体验。	美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.10 Maintenance (MA-1)
软件开发政策	通过列出需要遵循的所有协议和标准，使整个组织的软件开发实现标准化。		
系统和服务采购政策	提供用于评估、审查和验证系统及服务采购需求的程序。	美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.18 System and services acquisition (SA-1)

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
确保敏捷和可扩展的数字服务交付；指定组织可以与之合作的合作伙伴生态系统，或建立包含数字工厂、敏捷领导者和团队、持续流程和改进思维的双模式 IT 结构。		
建立开放、无偏见的文化，在研究潜在的新解决方案（不论内部构建还是购买）时公平、客观地评估备选方案。		

G. 组件：服务、基础设施和应用程序
• 数字工厂服务，将“快速 IT”（负责开发数字应用程序的数字工厂）与传统的核心 IT 分离 • 解决方案评估和选择服务 • 测试工具和服务

领域：内部构建、外部采购和实施 管理目标：BAI04 — 妥当管理的可用性和容量	焦点领域：COBIT 核心模型

描述

通过提供具有成本效益的服务来平衡当前和未来的可用性、性能和容量需求。包括评估当前能力、根据业务要求预测未来需求、分析业务影响和评估风险来计划和实施行动，从而满足已确定的需求。

目的

通过预测未来的性能和容量要求来维护服务可用性、有效的资源管理并优化系统性能。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化	AG05 提供符合业务需求的 I&T 服务

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG05	a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		

A. 组件：流程

管理实践	指标示例
BAI04.01 评估当前可用性、性能和能力并创建基准指标。 评估服务和资源的可用性、性能和容量，确保容量和性能的成本合理，从而支持业务需求和根据服务水平协议 (SLA) 交付服务和资源。创建可用性、性能和容量基准指标供未来对比之用。	a. 实际容量已用占比 b. 实际可用性占比 c. 实际性能占比

活动	能力级别
1. 评估服务和资源的可用性、性能和容量时考虑以下因素（当前的和预测的）：客户要求、业务优先级、业务目标、预算影响、资源利用率、IT 能力和行业趋势。	2
2. 确定和跟进所有因性能或容量不足而造成的事故。	3
3. 根据确定的阈值监控实际性能和容量使用情况，并在必要时使用自动化软件提供支持。	4
4. 根据趋势和 SLA 进行比较，对所有处理级别（业务需求、服务能力和资源容量）当前的性能水平进行定期评估。考虑环境变化。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	DP.CP Capacity Planning
ISF, The Standard of Good Practice for Information Security 2016	SY2.2 Performance and Capacity Management
ISO/IEC 20000-1:2011(E)	6.5 Capacity management
ITIL 第 3 版，2011 年	Service Design, 4.4 Availability Management; 4.5 Capacity Management
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.14 Planning (PL-10, PL-11)

A. 组件：流程（续）	
管理实践	**指标示例**
BAI04.02 评估业务影响。 确定对企业而言重要的服务。将服务和资源映射到业务流程中，并确定业务依赖关系。确保客户完全认同和接受不可用资源带来的影响。对于至关重要的业务功能，确保可根据服务水平协议 (SLA) 满足可用性要求。	a. 为评估未来的可用性情形而创建的场景数量 b. 已审批的分析结果的业务流程所有者的百分比

活动	能力级别
1. 仅识别那些在可用性和容量管理流程中非常重要的解决方案或服务。	2
2. 将所选择的解决方案或服务映射到它们所依赖的应用程序和基础设施（IT 和设施）中，以便能够聚焦于可用性计划的关键资源上。	3
3. 从过往故障和性能监控日志中收集可用性模式数据。使用建模工具，帮助根据新环境或用户状况的过往使用趋势和管理期望对故障进行预测。	4
4. 根据所收集的数据创建场景，描述未来可用性情形，从而说明实现可用性绩效目标所需的各种潜在容量水平。	
5. 根据场景，确定无法实现可用性绩效目标的可能性。	
6. 确定场景对业务绩效衡量指标（例如收益、利润、客户服务）的影响。接触业务线、职能（尤其是财务）和区域负责人，了解他们对影响的评价。	
7. 确保业务流程所有者充分了解和认同此分析的结果。从业务所有者那里获得不可接受的风险场景的列表，这些场景需要实施应对措施以将风险降至可接受的水平。	

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 20000-1:2011(E)	6.3 Service continuity and availability management

管理实践	指标示例
BAI04.03 计划新的或变更服务要求。 对更改业务需求和服务要求，在可用性、性能和容量影响等方面进行计划并确定优先级。	a. 计划外的容量、性能或可用性升级的数量 b. 管理层将实际的资源需求与预测的供需情况进行比较的百分比

活动	能力级别
1. 识别更改业务需求和改进机会对可用性和容量的影响。使用建模技术验证可用性、性能和容量计划。	3
2. 审查服务趋势分析的可用性和容量含义。	4
3. 确保管理层将实际的资源需求与预测的供需情况进行对比，从而评估当前的预测技术并尽可能做出改进。	
4. 确定所需改进的优先级并创建成本合理的可用性和容量计划。	5
5. 根据切实可行的、新的、建议的和/或预测的业务流程和支持性服务、应用程序和基础设施变更，来调整性能和容量计划以及 SLA。另外还包括审查实际性能和容量使用情况，包括负载水平。	

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 20000-1:2011(E)	5. 新服务或变更服务的设计和转换

管理实践	指标示例
BAI04.04 监控和审查可用性和容量。 监控、衡量、分析、报告和审查可用性、性能和容量。识别与已有基准指标的偏差。审查趋势分析报告，识别任何重大的问题和差异。在必要时采取行动，确保所有未决问题得到解决。	a. 超出计划容量限制的事件数量 b. 超过目标性能的交易峰值数量

A. 组件：流程（续）	
活动	**能力级别**
1. 为预算流程提供容量报告。	2
2. 建立数据收集流程，以便向管理层提供对所有 I&T 相关资源的可用性、性能和容量负载的监控和报告信息。	3
3. 定期以适当形式对结果进行报告，由 IT 和业务管理层审查并传达至企业管理层。	4
4. 将监控和报告活动整合到迭代容量管理活动中（监控、分析、调整和实施）。	
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	
管理实践	**指标示例**
BAI04.05 调查并解决可用性、性能和容量问题。 通过调查和解决已识别的可用性、性能和容量问题来应对偏差。	a. 未解决的可用性、性能和容量问题的数量和百分比 b. 可用性事故的数量
活动	**能力级别**
1. 利用供应商产品手册获取指导，为峰值处理和负载确保适当水平的性能可用性。	3
2. 确定升级上报程序，以便在发生紧急容量和性能问题时给予迅速解决。	
3. 通过监控当前的和预测的性能来界定性能和容量差距。使用已知的可用性、连续性和恢复规范对资源进行分类和确定优先级。	4
4. 确定纠正措施（例如，当界定出性能和容量问题时，转移负载、确定任务优先级或添加资源）。	5
5. 将所需的纠正措施整合到适当的计划中，并变更管理流程。	
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	

B. 组件：组织结构									
关键管理实践	**执行委员会**	**首席信息官**	**首席技术官**	**业务流程所有者**	**架构总监**	**IT 运营总监**	**服务经理**	**业务连续性经理**
BAI04.01 评估当前可用性、性能和能力并创建基准指标。		R	A	R		R	R	
BAI04.02 评估业务影响。	A			R		R	R	
BAI04.03 计划新的或变更服务要求。		R	A	R		R	R	
BAI04.04 监控和审查可用性和容量。	A			R		R	R	
BAI04.05 调查并解决可用性、性能和容量问题。		R	A	R	R	R	R	R
相关指南（标准、框架、合规性要求）	**详细参考**							
本组件没有相关指南								

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
BAI04.01 评估当前的可用性、性能和容量并创建基准指标。	自	描述	描述	至
	BAI02.01	需求定义贮存库	参照 SLA 进行的评估	APO09.05
	BAI02.03	需求风险登记表	可用性、性能和容量基准指标	内部
BAI04.02 评估业务影响。	BAI03.02	内部和外部服务水平协议 (SLA)	可用性、性能和容量业务影响评估	内部
			可用性、性能和容量场景	内部
BAI04.03 计划新的或变更服务要求。	BAI02.01	已确认的利益相关方验收标准	性能和容量计划	APO02.02
	BAI03.01	已批准的高层设计规范	已排定优先级的改进措施	APO02.02
	BAI03.02	已批准的详细设计规范		
	BAI03.03	记录的解决方案组件		
BAI04.04 监控和审查可用性和容量。			可用性、性能和容量监控审查报告	MEA01.03
BAI04.05 调查并解决可用性、性能和容量问题。			纠正措施	APO02.02
			紧急情况上报程序	DSS02.02
			性能和容量差距	内部

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
可用性管理	Skills Framework for the Information Age，第 6 版，2015 年	AVMT
容量管理	Skills Framework for the Information Age，第 6 版，2015 年	CPMG

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
可用性管理政策	通报基础设施可用性、可扩展性、可靠性和潜在恢复能力方面的规划。包括用于确定服务的带宽、容量和可用性（在设计和配置前）、制定服务水平协议 (SLA)、以及对电路、通信和响应时间实施持续监控的指引。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
对于信息服务企业来说，可用性和容量管理是成功运营的关键。企业所建立的文化应做到为产品和服务的可用性及容量排定优先级（与业务需求保持一致），并获得流程和行为的支持，这些流程和行为不仅能够在设计前确定所需的可用性和容量，在配置过程中也应加以考虑。以一致的方式定义明智的 SLA；持续监控电路、通信和响应时间；定期对业务连续性和基础设施的灾难恢复进行测试。		

G. 组件：服务、基础设施和应用程序
• 容量计划工具 • 配置服务和工具 • 服务水平监控工具

领域：内部构建、外部采购和实施 管理目标：BAI05 — 妥当管理的组织变更	焦点领域：COBIT 核心模型

描述

最大限度提高以更低的风险，快速、成功地实施可持续的企业级组织变更的可能性。覆盖变更的完整生命周期，以及业务及 IT 组织中所有受影响的利益相关方。

目的

为业务变更做好准备和承诺，减少失败的风险。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG05 以客户为中心的服务文化 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	• AG03 通过 I&T 促成的投资和服务组合所实现的效益 • AG08 通过集成应用程序和技术来推行和支持业务流程 • AG09 在预算内按时交付计划且满足要求和质量标准

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG03	a. 达到或超过业务案例宣称效益的 I&T 促成的投资的百分比 b. 实现预期效益（如服务水平协议所述）的 I&T 服务的百分比
EG05	a. 客户服务中断的次数 b. 业务利益相关方认为客户服务交付达到议定水平的百分比 c. 客户投诉的数量 d. 客户满意度调查结果的变化趋势	AG08	a. 执行业务服务或流程的时间 b. 因技术集成问题而延迟或产生额外成本的 I&T 促成的业务计划的数量 c. 因技术集成问题需要延迟或返工的业务流程变更的数量 d. 独立运行和未集成的应用程序或关键基础设施的数量
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度	AG09	a. 在预算内按时交付的计划/项目的数量 b. 因质量缺陷需要重大返工的计划的数量 c. 对计划/项目质量满意的利益相关方的百分比
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比		

A. 组件：流程

管理实践	指标示例
BAI05.01 树立变更愿望。 了解所需变更的范围和影响。评估利益相关方对变更的了解程度和意愿。确定可激励利益相关方接受和参与变更以提高变更成效的措施。	a. 高级管理层的参与程度 b. 利益相关方的变更意愿程度

A. 组件：流程（续）	
活动	**能力级别**
1. 评估预期的变更范围和影响、受影响的利益相关方、对每个利益相关方群体的影响性质及需要他们参与的程度，以及目前对于采纳变更的了解程度和能力。	2
2. 要树立变更愿望，需识别、利用和沟通当前的痛点、负面事件、风险、客户不满和业务问题，以及初步效益、未来的机会与奖励和竞争优势。	
3. 发布来自执行委员会或 CEO 的重要沟通信息，以表明变更决心。	
4. 高级管理层在设定方向，调解、激励和吸引利益相关方树立变更愿望等方面展现明确的领导意图。	
相关指南（标准、框架、合规性要求）	**详细参考**
PROSCI® 3-Phase Change Management Process	Phase 1. Preparing for change—Define your change management strategy
管理实践	**指标示例**
BAI05.02 成立有效的实施团队。 通过将合适的成员聚集在一起，彼此建立信任并制定共同目标和有效的衡量措施，建立有效的实施团队。	a. 实施团队中已确认技能或能力问题的数量 b. 相关利益方对实施团队的满意度评分
活动	**能力级别**
1. 确定并组建有效的核心实施团队，吸纳来自业务及 IT 组织、能够投入需要的时间量并贡献知识和专长、经验、信誉和权威的合适成员。考虑引入外部第三方（如顾问），以提供独立见解或弥补技术缺口。确定企业不同部门内潜在的变更推动者，核心团队可与他们合作以支持愿景和逐级推进变更。	3
2. 通过精心策划的活动开展有效的沟通和联合，在核心实施团队内建立相互信任。	
3. 制定支持企业目标的共同愿景和目标。	
相关指南（标准、框架、合规性要求）	**详细参考**
PROSCI® 3-Phase Change Management Process	Phase 1. Preparing for change—Prepare your change management team
管理实践	**指标示例**
BAI05.03 沟通预期愿景。 以受众的语言来沟通变更的预期愿景。应由高级管理层开展沟通，其中应包括变更的理由和益处；不进行变更的影响；以及各种利益相关方的愿景、路线图和需要的参与。	a. 与变更相关的问题数量 b. 利益相关方对于变更理解程度的反馈
活动	**能力级别**
1. 针对核心受众群体、他们的行为特征和信息需求、沟通渠道和原则，制定愿景沟通计划。	3
2. 根据该计划，在相应的企业层面开展沟通。	
3. 通过多次讨论和反复加强沟通。	
4. 让各级管理人员承担起呈现愿景的责任。	
5. 检查对于目标愿景的理解情况，回应员工重点关注的任何问题。	4
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
BAI05.04 为角色授权并确定速效方案。 通过分配责任为具有实施角色的人员授权。提供培训，并调整组织结构和人力资源流程。确定并沟通从推行变更的角度来看重要的速效方案。	a. 操作、使用和维护变更的角色的满意度 b. 受过培训的角色占比 c. 获得合适授权的角色占比 d. 角色对授权级别的反馈 e. 角色对相关能力的自我评估

活动	能力级别
1. 规划员工需要的培训机会，帮助他们培养适当的技能和心态来提升信心。	2
2. 识别、优化和交付速赢机会。这些机会可能与目前已知的迫切需要解决的难题或外部因素有关。	
3. 通过向受众说明愿景带来的好处，来实施速效方案。微调愿景，获得管理人员的继续支持并产生动力。	
4. 确定符合愿景需求的组织结构；如有必要，进行变更以确保符合愿景。	3
5. 协调 HR 流程和衡量体系（例如绩效评估、薪酬决策、晋升决定、招聘和雇用）来支持愿景。	
6. 对一直对抗必要变更的管理人员进行识别和管理。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
BAI05.05 启用操作和使用。 计划和实施技术、操作和使用的所有方面，让所有参与到未来状态环境中的人都可以履行他们的职责。	a. 获得适当的变更授权的用户占比 b. 为变更的运行和使用而制定的计划占比

活动	能力级别
1. 制定变更的运行作和使用计划。该计划应传达和扩充已实现的速效方案，解决实现更广泛过渡面临的文化和行为层面的问题，提升受众的支持和参与度。确保该计划涵盖关于变更的整体看法，并提供文档（如程序）、辅导、培训、指导、知识转移、更完善的上线后即时支持和持续支持。	3
2. 实施运行和使用计划。定义和跟踪成功衡量指标，包括硬性业务衡量指标，以及表明人们的变更感受的感性衡量指标。根据需要采取补救措施。	4

相关指南（标准、框架、合规性要求）	详细参考
PROSCI® 3-Phase Change Management Process	Phase 2. Managing change

管理实践	指标示例
BAI05.06 落实新方法。 通过跟踪变更实施、评估操作和使用计划的有效性，以及藉由定期沟通持续维持变更意识，来落实新方法。在适当的情况下采取纠正措施（可能包括合规强制性）。	a. 用户对变更采用情况的满意度 b. 识别出变更不力的根本原因的合规性审计占比 c. 为识别变更采用不力的根本原因而执行合规性审查并建议纠正措施的次数

活动	能力级别
1. 让流程所有者承担起日常操作的责任。	2
2. 庆祝成功，实施奖励和表彰计划，以巩固变更效果。	3
3. 通过定期沟通变更及其采用情况，持续提升变更意识。	
4. 使用绩效衡量系统识别采用不力的根本原因。采取纠正措施。	4
5. 进行合规性审计，确定采用不力的根本原因。建议纠正措施。	

相关指南（标准、框架、合规性要求）	详细参考
PROSCI® 3-Phase Change Management Process	Phase 3. Reinforcing change

A. 组件：流程（续）	
管理实践	**指标示例**
BAI05.07 维持变更。 通过有效地培训新员工、持续开展沟通活动、持续获得最高管理层的承诺，以及在整个企业范围内监控采用情况和分享经验教训，来维持变更的执行。	a. 进行的培训和知识转移的数量 b. 最高管理层参与巩固变更的百分比

活动	能力级别
1. 通过定期沟通展示最高管理层的决心，维持和巩固变更。	2
2. 为新员工提供辅导、培训、指导和知识转移，以维持变更的执行。	3
3. 定期审查变更的操作和使用情况。确定需要改进之处。	4
4. 吸取与变更实施相关的经验教训。在整个企业中分享知识。	5

相关指南（标准、框架、合规性要求）	详细参考
PROSCI® 3-Phase Change Management Process	Phase 3. Reinforcing change

B. 组件：组织结构

关键管理实践	执行委员会	首席执行官	首席运营官	首席信息官	首席技术官	首席数字官	I&T 治理委员会	业务流程所有者	计划经理	项目经理	项目管理办公室	人力资源总监	开发总监	IT 运营总监	服务经理	信息安全经理	业务连续性经理
BAI05.01 树立变更愿望。	R	A		R	R	R	R	R	R	R		R					
BAI05.02 成立有效的实施团队。	A			R	R	R			R	R	R		R				
BAI05.03 沟通预期愿景。	A			R	R	R	R		R	R							
BAI05.04 为角色授权并确定速效方案。	A			R	R	R			R	R		R					
BAI05.05 启用操作和使用。	A		R	R	R	R		R			R		R	R	R	R	R
BAI05.06 落实新方法。	A		R	R	R	R		R			R		R	R	R	R	R
BAI05.07 维持变更。	A		R	R	R	R		R	R	R	R		R	R	R	R	R

相关指南（标准、框架、合规性要求）
本组件没有相关指南

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
BAI05.01 树立变更愿望。	APO11.02	服务质量的结果，包括客户反馈	执行管理层传达变更承诺	内部
	BAI02.01	• 需求定义贮存库 • 利益相关方已确认的验收标准	变更驱动因素的沟通	内部
	BAI02.03	• 需求风险登记表 • 风险缓解措施		
	BAI03.01	已批准的高层设计规范		
	BAI03.02	已批准的详细设计规范		
BAI05.02 成立有效的实施团队。	BAI02.01	已确认的利益相关方验收标准	共同愿景和目标	BAI01.02
			实施团队和角色	BAI01.04
BAI05.03 沟通预期愿景。			愿景沟通计划	BAI01.04
			愿景沟通	BAI01.05
BAI05.04 为角色授权并确定速效方案。	在 COBIT 外部	企业组织结构	调整的 HR 绩效目标	APO07.04
			已确定的速效方案	BAI01.04
			效益沟通	BAI01.06
BAI05.05 启用操作和使用。	BAI03.03	记录的解决方案组件	操作和使用计划	APO08.04；BAI08.03；DSS01.01；DSS01.02；DSS06.02
	BAI03.10	更新的解决方案组件和相关的文档	成功衡量指标和结果	APO08.05；BAI07.07；BAI07.08；MEA01.03
BAI05.06 落实新方法。			HR 绩效审查结果	APO07.04
			意识沟通	内部
			合规性审计结果	MEA02.02；MEA03.03
BAI05.07 维持变更。			知识转移计划	BAI08.02；BAI08.03
			传达管理层承诺	内部
			操作使用情况的审查	MEA02.02
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
业务变更管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage—E.7. Business Change Management
变更实施计划和管理	Skills Framework for the Information Age，第 6 版，2015 年	CIPM
组织设计和实施	Skills Framework for the Information Age，第 6 版，2015 年	ORDI

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
组织变更管理政策	为管理组织变更提供框架并规定原则纲要。反映现行法规，并提供良好的人事管理实践；确保整个组织内执行一致的变更管理方法。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
要实现 I&T 投资收益，仅仅交付 I&T 解决方案和服务是不够的，还需要变更业务流程、技能与能力、文化和行为等，所有这些都必须包括在投资业务案例中。领导层必须营造灵活、开放和自信的持续变更文化，并建立适当的变更管理支持和沟通。		

G. 组件：服务、基础设施和应用程序
• 沟通工具和渠道 • 调查工具

领域：内部构建、外部采购和实施 管理目标：BAI06 — 妥当管理的 IT 变更	焦点领域：COBIT 核心模型

描述

以受控制的方式管理所有变更，包括与业务流程、应用程序和基础设施相关的标准变更和紧急维护。这包括变更标准和程序、影响评估、确定优先级和授权、紧急变更、跟踪、报告、关闭和记录。

目的

快速、可靠地交付业务变更。缓解对变更后环境的稳定性或完整性产生负面影响的风险。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标		一致性目标
EG01 有竞争力的产品和服务的组合	→	AG06 将业务需求转化为可运作的解决方案的敏捷性
企业目标的指标示例		**一致性目标的指标示例**
EG01 a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间		AG06 a. 业务高管对 I&T 响应新需求的满意度水平 b. 新的 I&T 相关服务和应用程序的平均上市时间 c. 将战略 I&T 目标转化为议定的已批准举措所需的平均时间 d. 受最新基础设施和应用支持的关键业务流程的数量

A. 组件：流程

管理实践	指标示例
BAI06.01 评估、优先级排序和授权变更请求。 评估所有变更请求，以确定对业务流程和 I&T 服务的影响，以及评估变更是否会对运营环境造成不利影响并引入不可接受的风险。确保对变更进行记录、排定优先级、归类、评估、授权、计划和日程计划安排。	a. 变更失败导致的返工量 b. 由于影响评估不充分导致的失败变更的百分比

活动	能力级别
1. 使用正式的变更请求，允许业务流程所有者和 IT 请求变更业务流程、基础设施、系统或应用程序。确保所有此类变更仅通过变更请求管理流程进行。	2
2. 对所有变更请求进行分类（例如业务流程、基础设施、操作系统、网络、应用程序系统、采购/打包的应用程序软件），并关联受影响的配置项。	
3. 根据业务及技术要求、所需资源，以及请求变更的法律、法规和合同原因，排定所有变更请求的优先级。	
4. 在适当情况下，由业务流程所有者、服务经理和 IT 技术相关利益方正式批准每项变更。低风险且相对频繁的变更应预先批准为标准变更。	
5. 计划和安排所有批准的变更。	
6. 以结构化方式计划和评估所有变更请求。提供变更对业务流程、基础设施、系统及应用程序、业务连续性计划 (BCP) 和服务提供商的影响分析，以确保识别所有受影响的组件。评估对运营环境产生不利影响的可能性，以及实施变更带来的风险。考虑请求的变更带来的安全、隐私、法律、合同及合规性影响。还要考虑变更之间的相互依赖性。适当情况下，让业务流程所有者参与到评估流程中。	3
7. 考虑外包服务提供商（如已外包的业务处理、基础设施、应用程序开发和共享服务的提供商）对变更管理流程的影响。包括组织变更管理流程与服务提供商变更管理流程的整合，以及对合同条款和 SLA 的影响。	

相关指南（标准、框架、合规性要求）	详细参考
ISF, The Standard of Good Practice for Information Security 2016	SY2.4 Change Management
ISO/IEC 20000-1:2011(E)	9.2 Change management
ITIL 第 3 版，2011 年	Service Transition, 4.2 Change Management
PMBOK Guide，第 6 版，2017 年	Part 1: 4.6 Perform Integrated Change Control

A. 组件：流程（续）	
管理实践	**指标示例**
BAI06.02 管理紧急变更。 认真管理紧急变更，最大限度减少后续事故的发生。确保以安全、受控的方式执行紧急变更。确认紧急变更在执行后进行了适当的评估并获得授权。	a. 事故后未获授权的紧急变更的数量 b. 紧急修复占总变更数的百分比

活动	能力级别
1. 定义紧急变更的构成要素。	2
2. 确保存在关于紧急变更申报、评估、初步审批、事后授权和记录的书面程序。	
3. 确认针对变更的所有应急访问安排都已得到适当授权、记录并且在实施变更后予以撤销。	3
4. 监控所有紧急变更，所有相关各方参与实施后审查。审查时基于根本原因（例如业务流程、应用程序系统开发及维护、开发与测试环境、文档及手册和数据完整性等方面存在的问题），考虑和发起纠正措施。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
BAI06.03 跟踪和报告变更状态。 维护跟踪与报告系统来记录被拒绝的变更，沟通已批准、进行中和已完成的变更的状态。确保按计划实施获得批准的变更。	a. 积压的变更请求的数量和时间 b. 及时向利益相关方报告变更请求状态的百分比

活动	能力级别
1. 在跟踪流程中对变更请求进行分类（例如被拒绝、获得批准但尚未启动、已批准且正在进行和已关闭）。	4
2. 按绩效指标制定变更状态报告，使管理层能够审查和监控详细的变更状态和总体状况（例如过往的变更请求分析）。确保利用状态报告形成审计轨迹，以便后续能够从始至终跟踪变更。	
3. 监控待处理的变更，确保根据优先级及时关闭所有已批准的变更。	
4. 维护针对所有变更请求的跟踪与报告系统。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	IP.CC Apply Change Control

管理实践	指标示例
BAI06.04 关闭并记录变更。 任何时候在实施变更后，更新受变更影响的解决方案、用户文档及程序。	a. 在文档中发现的审查错误的数量 b. 用户文档和程序及时执行更新的百分比

活动	能力级别
1. 在管理程序中包含变更文档。文档示例包括业务及 IT 运营程序、业务连续性与灾难恢复文档、配置信息、应用程序文档、帮助屏幕和培训材料。	2
2. 为变更文档、变更前和变更后的系统和用户文档定义适当的保留期限。	3
3. 对文档与实际变更进行相同级别的审查。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构										
关键管理实践	首席信息官	业务流程所有者	计划经理	项目经理	开发总监	IT 运营总监	服务经理	信息安全经理	业务连续性经理	隐私官
BAI06.01 评估、优先级排序和授权变更请求。	A	R			R	R	R	R	R	R
BAI06.02 管理紧急变更。	A				R	R	R	R		R
BAI06.03 跟踪和报告变更状态。	A	R	R	R	R	R	R			
BAI06.04 关闭并记录变更。	A	R	R	R	R	R	R		R	

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
BAI06.01 评估、优先级排序和授权变更请求。	BAI03.05	已集成和配置的解决方案组件	变更计划和时间安排	BAI07.01
	DSS02.03	已批准的服务请求	已批准的变更请求	BAI07.01
	DSS03.03	针对已知错误建议的解决方案	影响评估	内部
	DSS03.05	确定的可持续的解决方案		
	DSS04.08	已批准的计划变更		
	DSS06.01	根本原因分析和建议		
BAI06.02 管理紧急变更。			紧急变更的实施后审查	内部
BAI06.03 跟踪和报告变更状态。	BAI03.09	所有已批准和应用的变更请求的记录	变更请求状态报告	BAI01.06; BAI10.03
BAI06.04 关闭并记录变更。			变更文档	内部

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
变更管理	Skills Framework for the Information Age，第 6 版，2015 年	CHMG
变更支持	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	C. Run - C.2. Change Support

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
IT 变更管理政策	传达管理层意图，确保企业 IT 的所有变更都得到妥当管理和实施，以最大限度降低风险并减少对利益相关方的影响。涵盖范围内资产和标准变更管理流程。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
管理层必须建立持续改进 IT 解决方案和服务的文化，认识到这类改进需要他们理解技术变更对企业的影响、其固有的风险和相关缓解措施及其成本。管理层必须考虑变更的影响与其预期效益和对 I&T 战略及企业目标的贡献之间的平衡。		

G. 组件：服务、基础设施和应用程序
• 配置管理工具 • IT 变更管理工具

领域：内部构建、外部采购和实施 管理目标：BAI07 — 妥当管理的 IT 变更接受和交接	焦点领域：COBIT 核心模型

描述

正式接受并制定可操作的全新解决方案，包括实施规划、系统和数据转换、验收测试、沟通、发布准备、促进产生新的或变更的业务流程和 I&T 服务、早期生产支持和实施后审查。

目的

根据协定的期望和成果，安全地实施解决方案。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标		一致性目标
EG01 有竞争力的产品和服务的组合	→	AG06 将业务需求转化为可运作的解决方案的敏捷性
企业目标的指标示例		**一致性目标的指标示例**
EG01 a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间		AG06 a. 业务高管对 I&T 响应新需求的满意度水平 b. 新的 I&T 相关服务和应用程序的平均上市时间 c. 将战略 I&T 目标转化为议定的已批准举措所需的平均时间 d. 受最新基础设施和应用支持的关键业务流程的数量

A. 组件：流程

管理实践	指标示例
BAI07.01 建立实施计划。 建立实施计划，涵盖系统和数据转换、验收测试衡量标准、沟通、培训、发布准备、推广到生产、早期生产支持、回退/备用计划以及实施后审查。获得相关方的批准。	a. 签字批准实施计划的利益相关方的数量和类别 b. 可靠且包含所有必要组件的实施计划的数量

活动	能力级别
1. 创建实施计划，该计划应反映总体实施战略、实施步骤的顺序、资源需求、相互依存关系、管理层对生产实施的验收标准、安装验证要求、生产支持的过渡战略以及业务连续性计划的更新。	2
2. 获取外部解决方案提供商对其参与的各个实施步骤的承诺。	
3. 识别并记录回退和恢复流程。	
4. 确认所有实施计划均已获得技术和业务利益相关方的批准和内部审计的审查（如适用）。	3
5. 正式审查与实施相关的技术和业务风险。确保规划流程已考虑并解决关键风险。	

相关指南（标准、框架、合规性要求）	详细参考
ITIL 第 3 版，2011 年	Service Transition, 4.1 Transition Planning and Support

A. 组件：流程（续）	
管理实践	**指标示例**
BAI07.02 计划业务流程、系统和数据转换。 作为企业开发方法的一部分，准备业务流程、I&T 服务数据和基础设施迁移，包括审计轨迹和迁移失败时的恢复计划。	a. 转换的成功率 b. 接受必要调整的程序的百分比（包括修改角色和职责以及控制程序）

活动	能力级别
1. 定义业务流程、I&T 服务数据和基础设施迁移计划。制定计划时，应考虑硬件、网络、操作系统、软件、交易数据、主文件、备份和归档、与其他系统（内部和外部）之间的接口、可能的合规性要求、业务程序和系统文档等方面。	2
2. 业务流程转换计划应考虑所有必要的程序调整，包括修改角色和职责以及控制程序。	
3. 确认数据转换计划无需更改数据值，除非因为业务原因更改实属必要。记录对数据值所做的更改，并确保获取业务流程数据所有者的批准。	
4. 做好备份和归档数据的保留计划，以符合业务需求以及监管或合规性要求。	
5. 在尝试实际转换之前，应进行转换练习和测试。	
6. 协调并验证进行转换切换的时机和完整性，确保在不丢失任何交易数据的情况下实现平稳、持续的过渡。在没有任何其他备选方案的情况下，可在必要时暂停现场运行。	
7. 做好在转换之前备份所有相关系统和数据的计划。维护审计轨迹以确保转换能够追溯。确保已制定涵盖迁移回滚以及迁移失败时回退到先前处理状态的恢复计划。	
8. 数据转换计划应包含收集、转换和验证待转换数据以及识别和解决转换期间发现的任何错误的方法，包括比较原始数据和转换后数据的完备性和完整性。	3
9. 考虑发生转换问题的风险；业务流程中的业务连续性规划和回退程序；包含风险管理、业务需求或监管/合规要求的数据和基础设施迁移计划。	

相关指南（标准、框架、合规性要求）	详细参考
ITIL 第 3 版，2011 年	Service Transition, 4.1 Transition Planning and Support

管理实践	指标示例
BAI07.03 计划验收测试。 基于定义角色、职责和进出条件的企业级标准建立测试计划。确保计划得到相关方的批准。	a. 对测试流程的完整性满意的利益相关方的百分比 b. 包含所有测试阶段和可靠测试情景且适合运营要求和环境的书面测试计划的数量

A. 组件：流程（续）	
活动	**能力级别**
1. 制定并记录与计划、项目质量计划和相关组织标准保持一致的测试计划。与相应的业务流程所有者和 IT 利益相关方进行沟通和磋商。	2
2. 确保测试计划反映项目的风险评估，并确保对所有功能和技术要求进行测试。基于对系统故障和实施相关故障进行的风险评估，将性能、压力、可用性、试点、安全测试和隐私等方面的要求纳入计划。	
3. 确保测试计划满足内部或外部对测试流程成果的潜在鉴定需求（如财务或监管要求）。	
4. 确保测试计划确定在执行测试和评估结果时所需的资源。资源示例可能包括测试环境的构建和占用的测试组人员的时间，包括可能需要临时替换生产或开发环境中的测试人员。确保就测试计划的资源影响与利益相关方进行磋商。	
5. 确保测试计划确定适合运营要求和环境的测试阶段。此类测试阶段的示例包括单元测试、系统测试、集成测试、用户验收测试、性能测试、压力测试、数据转换测试、安全测试、隐私测试、操作就绪测试以及备份和恢复测试。	
6. 确认测试计划已考虑测试准备（包括现场准备）、培训要求、既定测试环境的安装或更新、规划/执行/记录/保留测试案例、错误和问题处理、纠正和上报以及正式批准。	
7. 确认所有测试计划均已获得利益相关方（包括业务流程所有者和 IT 相关方）的批准（如适用）。利益相关方可能包括应用程序开发经理、项目经理和业务流程最终用户。	
8. 确保测试计划已针对所开展的各个测试阶段制定明确的成功衡量标准。定义成功的衡量标准时，与业务流程所有者和 IT 利益相关方进行磋商。确定计划已制定未满足成功衡量标准时的补救程序。例如，如果某个测试阶段发生重大故障，计划应该就继续下一阶段、停止测试还是推迟实施提供相关指导。	3
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	
管理实践	**指标示例**
BAI07.04 建立测试环境。 定义和建立安全的测试环境，该环境应该能够在性能、容量、安全、内部控制、操作实践、数据质量和隐私要求以及工作量等方面代表计划的业务流程和 IT 操作环境。	a. 测试环境与未来的业务和运营环境之间的可比性水平 b. 经过清理的测试数据（和/或数据库）能够代表生产环境的程度
活动	**能力级别**
1. 创建能代表生产环境的测试数据数据库。根据业务需求和组织标准，从生产环境中清理测试环境所用的数据。例如，考虑合规或监管要求是否要求使用经过清理的数据。	2
2. 保护敏感的测试数据和结果在访问、保留、存储和销毁等过程中不被泄露。考虑组织系统与第三方系统之间的交互所产生的影响。	3
3. 妥善实施能够正确保留或处理测试结果、介质和其他相关文档的流程，以便根据测试计划的要求进行充分审查和后续分析或执行有效的重新测试。考虑监管或合规性要求的影响。	
4. 确保测试环境能代表未来的业务和运营环境，包括生产环境中存在的业务流程程序和角色、可能的工作量压力、操作系统、必要的应用程序软件、数据库管理系统以及网络和计算基础设施。	
5. 确保测试环境不仅安全，而且也无法与生产系统进行交互。	
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
BAI07.05 执行验收测试。 在迁移到现场操作环境之前，根据既定测试计划对变更进行独立测试。	a. 在验收测试结果与既定的成功衡量标准之间识别的差距数量 b. 成功实施的验收测试的数量

活动	能力级别
1. 审查开发团队在测试流程中发现的经过分类的错误日志。验证是否所有错误均已得到补救或被正式接受。	2
2. 根据成功的衡量标准评估最终验收，并解释最终验收测试的结果。以业务流程所有者和 IT 人员可以理解的形式呈现结果，以便开展知情审查和评估。	3
3. 在推广之前，由业务流程所有者、第三方（如适用）和 IT 利益相关方正式签字批准验收。	
4. 确保根据测试计划执行变更测试。确保由独立于开发团队的测试组来设计和执行测试。考虑业务流程所有者和最终用户在测试组的参与程度。确保仅在测试环境中执行测试。	
5. 确保测试和预期成果符合测试计划中规定的成功衡量标准。	
6. 考虑使用明确定义的测试说明（脚本）执行测试。确保由独立测试组对每个测试脚本进行评估和批准，以确认脚本充分满足测试计划中规定的测试成功标准。考虑使用脚本来验证系统满足安全和隐私要求的程度。	
7. 考虑在自动化脚本测试和交互式用户测试之间取得适当平衡。	
8. 根据测试计划执行安全测试。衡量安全弱点或漏洞的范围。考虑自测试计划构建以来发生的安全事故产生的影响。考虑对访问控制和边界控制的影响。考虑隐私。	
9. 根据测试计划执行系统和应用程序性能测试。考虑一系列的性能指标（如最终用户响应时间和数据库管理系统更新性能）。	
10. 进行测试时，确保已妥善应对测试计划的回退和回滚元素。	
11. 识别和记录测试期间出现的错误并进行分类（如次要、重要、关键任务错误）。确保提供测试结果的审计轨迹。根据测试计划将测试结果传达给利益相关方，以促进错误修复并进一步提高质量。	

相关指南（标准、框架、合规性要求）	详细参考
ITIL 第 3 版，2011 年	Service Transition, 4.5 Service Validation and Testing

管理实践	指标示例
BAI07.06 推广到生产和管理发布。 将验收的解决方案推广到业务和运营当中。适当情况下，以试点实施的形式运行解决方案，或在规定的时期内与旧解决方案并行运行并且比较行为和结果。如果出现重大问题，则根据回退/备份计划恢复到原始环境。管理解决方案组成部分的发布。	a. 未准备好按日程安排发布的发布数量和百分比 b. 利益相关方对所实施解决方案的满意度

活动	能力级别
1. 根据组织变更管理标准，做好将业务程序和支持性服务、应用程序和基础设施从测试环境转移到生产环境的准备。	2
2. 根据实施计划确定试点实施或新旧系统并行处理的范围。	
3. 及时更新相关业务流程和系统文档、配置信息和应急计划文档（如适用）。	
4. 确保将正在从测试环境转移到生产环境的解决方案组件版本及时更新到所有介质库。将现有版本及其支持文件归档。确保依据配置控制，将系统、应用程序软件和基础设施推广到生产环境。	
5. 如果以电子方式分发解决方案组件，则应控制自动分发过程，确保用户收到通知，并且仅向获得授权和正确识别的目标地点进行分发。发布流程中应包含备份程序，以便在发生故障或错误时对变更的分发进行审查。	
6. 如果采用物理形式分发，则应保存正式日志，记录已分发的项目、分发对象、项目的实施地点和各自的更新时间。	

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
ISO/IEC 20000-1:2011(E)	9.3 Release and deployment management
ITIL V3 2011	Service Transition, 4.4 Release and Deployment Management
管理实践	**指标示例**
BAI07.07 提供早期产品支持。 在商定的期限内，为用户和 I&T 运营提供早期支持，以解决问题并为新解决方案的稳定实施提供帮助。	a. 参与支持的额外 I&T 系统资源的数量 b. 参与支持的额外人力资源的数量
活动	**能力级别**
1. 视需要为最终用户和支持人员提供额外资源，直到发布达到稳定状态。	3
2. 视需要提供额外的 I&T 系统资源，直到发布处于稳定的操作环境中。	
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	
管理实践	**指标示例**
BAI07.08 执行实施后审查。 开展实施后审查，以确认成果和结果，确定经验教训并制定行动计划。对照用户或客户预计的性能和成果预期，评估新服务或变更后的服务的实际性能和成果。	a. 已完成的根本原因分析的数量和百分比 b. 未在可接受期限内达到稳定的发布数量或百分比 c. 导致停机的发布所占的百分比
活动	**能力级别**
1. 制定相应的程序，确保实施后审查能够识别、评估和报告以下事件的进展程度：企业要求得到满足；预期效益得到实现；系统被视为可用；内部和外部利益相关方的期望得到满足；对企业产生意外影响；关键风险得到缓解；以及变更管理、安装和认证流程均得到有效和高效地执行。	3
2. 与业务流程所有者和 IT 技术管理人员磋商，选择用于衡量需求与效益的成功及实现的衡量指标。	4
3. 根据组织变更管理流程执行实施后审查。让业务流程所有者和第三方参与（如适用）。	
4. 考虑因外部业务和 IT（如内部审计、ERM、合规性）引起的实施后审查需求。	
5. 商定并实施行动计划，以解决在实施后审查中发现的问题。在制定行动计划时让业务流程所有者和 IT 技术管理人员参与其中。	5
相关指南（标准、框架、合规性要求）	**详细参考**
ITIL 第 3 版，2011 年	Service Transition, 4.6 Change Evaluation

B. 组件：组织结构										
关键管理实践	首席信息官	业务流程所有者	数据管理职能部门	开发总监	IT 运营总监	服务经理	信息安全经理	业务连续性经理	隐私官
BAI07.01 建立实施计划。	A	R		R		R	R	R	
BAI07.02 计划业务流程、系统和数据转换。	A	R	R	R		R	R	R	
BAI07.03 计划验收测试。	A	R		R	R		R	R	R
BAI07.04 建立测试环境。	A	R		R	R		R	R	
BAI07.05 执行验收测试。	A	R		R	R		R	R	R
BAI07.06 推广到生产和管理发布。	A	R		R	R	R		R	
BAI07.07 提供早期产品支持。	A	R		R	R	R			
BAI07.08 执行实施后审查。	A	R		R	R	R			

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
BAI07.01 建立实施计划。	BAI01.07	质量管理计划	实施回退和恢复流程	内部
	BAI06.01	• 经批准的变更请求 • 变更计划和时间表	经批准的实施计划	内部
	BAI11.05	项目质量管理计划		
BAI07.02 计划业务流程、系统和数据转换。			迁移计划	DSS06.02
BAI07.03 计划验收测试。	BAI01.07	可交付成果的独立验证要求	已批准的验收测试计划	BAI01.04；BAI11.04
	BAI03.07	• 测试计划 • 测试程序		
	BAI03.08	• 测试结果日志和审计轨迹 • 测试结果沟通		
	BAI11.05	项目交付成果的独立验证要求		

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
BAI07.04 建立测试环境。	**自**	**描述**	**描述**	**至**
			测试数据	内部
BAI07.05 执行验收测试。			经批准的验收和生产发布	BAI01.04
			验收结果的评估	BAI01.06
			测试结果日志	内部
BAI07.06 推广到生产和管理发布。			发布计划	BAI10.01
			发布日志	内部
BAI07.07 提供早期产品支持。	APO11.02	服务质量的结果，包括客户反馈	补充性支持计划	APO08.04；APO08.05；DSS02.04
	BAI05.05	成功衡量指标和结果		
BAI07.08 执行实施后审查。	APO11.03	• 解决方案和服务交付质量监控的结果 • 交付质量失败的根本原因	补救行动计划	BAI01.09；BAI11.09
	APO11.04	质量审查和审计的结果	实施后审查报告	BAI01.09；BAI11.09
	BAI05.05	成功衡量指标和结果		
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
业务流程测试	Skills Framework for the Information Age，第 6 版，2015 年	BPTS
发布和部署	Skills Framework for the Information Age，第 6 版，2015 年	RELM
服务验收	Skills Framework for the Information Age，第 6 版，2015 年	SEAC
测试	Skills Framework for the Information Age，第 6 版，2015 年	TEST
用户体验评估	Skills Framework for the Information Age，第 6 版，2015 年	USEV

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
IT 变更管理政策	传达管理层意图，确保企业 IT 的所有变更都得到妥当管理和实施，以最大限度降低风险并减少对利益相关方的影响。涵盖范围内资产和标准变更管理流程。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
建立确保及时向受影响群体传达 IT 变更请求的文化；就变更的实施和测试与受影响的群体进行磋商。		

G. 组件：服务、基础设施和应用程序
• IT 变更管理工具 • 发布管理工具 • 测试工具和服务

领域：内部构建、外部采购和实施 管理目标：BAI08 — 妥当管理的知识	焦点领域：COBIT 核心模型

描述

维护相关、现势、已验证且可靠的知识及管理信息的可用性来支持所有的流程活动并促进与企业 I&T 的治理和管理有关的决策。制定关于识别、收集、组织、维护、使用和废弃知识的计划。

目的

为所有员工提供支持企业 I&T 治理和管理以及作出明智决策所需的知识和信息。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG10 员工技能、动力和生产力 • EG13 产品和业务创新	• AG12 既了解技术又熟知业务、能力出众且积极上进的员工 • AG13 业务创新的知识、专业技能和举措

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG12	a. 精通 I&T 的业务人员（即具备必要的 I&T 知识且了解 I&T，能够引导、指导、创立和发现在其业务专业领域运用 I&T 的机会）的百分比 b. 精通业务的 I&T 人员（即具备必要的相关业务领域知识和理解，能够引导、指导、创立和发现在业务领域运用 I&T 的机会）的百分比 c. 拥有技术管理经验的业务人员的数量或百分比
EG10	a. 相较于基准的员工生产力 b. 利益相关方对员工专业知识和技能的满意度 c. 相对其角色所需能力而言技能不足的员工的百分比 d. 满意员工的百分比	AG13	a. 业务高管对 I&T 创新可能性的认识和理解水平 b. 源自 I&T 创新想法的已批准举措的数量 c. 获得认可/奖励的创新推动者的数量
EG13	a. 对业务创新机会的认识和理解水平 b. 利益相关方对产品以及创新专长和想法的满意度 c. 源自创新想法的已批准产品和服务举措的数量		

A. 组件：流程	
管理实践	**指标示例**
BAI08.01 识别 I&T 治理和管理的信息来源并对其进行分类。 识别和验证实现 I&T 治理和管理所需的内外部信息来源并对其进行分类，包括战略文档、事故报告以及上线之前从开发推进到运营的配置信息。	a. 已分类信息得到验证的百分比 b. 内容类型、构件以及结构化信息和非结构化信息的适宜性百分比

活动	能力级别
1. 识别潜在的知识用户，包括可能需要贡献和批准知识的信息所有者。获取已识别用户的知识要求和信息来源。	2
2. 考虑内容类型（程序、流程、结构、概念、政策、规定、事实、分类）、构件（文档、记录、视频、语音）、结构化和非结构化信息（专家、社交媒体、电子邮件、语音邮件、丰富站点摘要 (RSS) 馈送）。	
3. 根据内容分类方案（如信息架构模型）对信息来源进行分类。将信息来源对应到分类方案。	3
4. 根据信息验证标准（如可理解性、关联性、重要性、完整性、准确性、一致性、机密性、现势性和可靠性）收集、核对并验证信息来源。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
BAI08.02 将信息组织起来，并将其转化为知识。 根据分类标准组织信息。识别和创建信息元素之间有意义的关系，并实现信息的使用。识别管理信息和知识资源的所有者，并运用和实施企业定义的信息访问级别。	a. 信息来源中已识别的关系数量（标记） b. 对组织信息并将信息转化为知识感到满意的利益相关方的百分比

活动	能力级别
1. 识别共享属性并匹配信息来源，在信息集中创建关系（信息标记）。	3
2. 考虑利益相关方和组织的要求，创建相关数据集的视图。	
3. 设计和实施相关方案，以便对通过正式来源无法获得的非结构化知识（如专家知识）进行管理。	
4. 根据角色和访问机制，向相关的利益相关方发布和提供知识。	

相关指南（标准、框架、合规性要求）	详细参考
COSO Enterprise Risk Management，2017 年 6 月	10. Information, Communication, and Reporting - Principle 18

管理实践	指标示例
BAI08.03 使用和共享知识。 将可用的知识资源传播到相关的利益相关方并沟通如何使这些资源满足不同的需求（例如，解决问题、学习、战略计划和决策等）。	a. 可用知识被实际使用的百分比 b. 令用户满意的知识的百分比

活动	能力级别
1. 针对知识的有用性以及分享企业 I&T 治理和管理相关知识的需求，设定管理期望并表明相应的态度。	2
2. 通过知识分类识别潜在的知识用户。	
3. 根据需求差距分析和有效的学习手段，将知识转移给知识用户。创建能够为知识共享和转移提供支持的环境、工具和构件。确保已妥善实施符合既定知识分类的适当访问控制。	3
4. 衡量知识工具和要素的使用情况，并评估其对治理流程的影响。	4
5. 为展示知识差距的治理流程改善信息和知识。	5

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI Cybermaturity Platform，2018 年	PP.IS Apply Information Sharing; IR.ES Ensure Information sharing
ITIL 第 3 版，2011 年	Service Transition, 4.7 Knowledge Management
PMBOK Guide，第 6 版，2017 年	Part 1: 4.4 Manage project knowledge
管理实践	**指标示例**
BAI08.04 评估和更新或停用信息。 衡量信息的使用情况并对信息的现势性和相关性进行评估。更新信息或停用过时的信息。	a. 更新的频率 b. 用户的满意度

活动	能力级别
1. 定义知识停用控制并据此停用相应的知识。	3
2. 评估知识要素的实用性、相关性和价值。更新仍对组织具有相关性和价值的过时信息。识别与企业的知识需求不再相关的相关信息，并根据政策予以停用或归档。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构

关键管理实践	首席信息官	首席技术官	首席数字官	业务流程所有者	组合经理	计划经理	项目经理	数据管理职能部门	架构总监	开发总监	IT 运营总监	IT 行政总监	服务经理	信息安全经理	业务连续性经理	隐私官	法律顾问
BAI08.01 识别 I&T 治理和管理的信息来源并对其进行分类。	A			R				R		R	R		R				
BAI08.02 将信息组织起来，并将其转化为知识。	A							R		R	R	R					
BAI08.03 使用和共享知识。	A	R	R	R	R	R	R	R				R					R
BAI08.04 评估和更新或停用信息。	A			R		R	R	R	R	R	R	R	R	R	R	R	

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
BAI08.01 识别 I&T 治理和管理的信息来源并对其进行分类。	在 COBIT 外部	知识需求和来源	信息来源分类	内部
BAI08.02 将信息组织起来，并将其转化为知识。	BAI03.03	记录的解决方案组件	已发布的知识贮存库	APO07.03
	BAI05.07	知识转移计划		
BAI08.03 使用和共享知识。	BAI03.03	记录的解决方案组件	知识意识和培训方案	APO07.03
	BAI05.05	操作和使用计划	知识用户数据库	内部
	BAI05.07	知识转移计划		
BAI08.04 评估和更新或停用信息。			知识停用规则	内部
			知识使用情况的评估结果	内部

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
信息和知识管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	D. Enable—D.10. Information and Knowledge Management

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
治理知识使用政策	为创建和使用与 I&T 治理相关的知识资产提供指导。I&T 知识资产应易于获取以供参考。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
在企业中落实知识共享文化。主动传达知识的价值，以鼓励知识的创造、使用、重复使用和共享。通过识别和利用激励因素来鼓励知识共享和转移。		

G. 组件：服务、基础设施和应用程序
• 协作平台 • 知识贮存库

领域：内部构建、外部采购和实施 管理目标：BAI09 — 妥当管理的资产	焦点领域：COBIT 核心模型

描述

管理 I&T 资产贯穿其生命周期，以确保该资产的使用达到了最佳成本效益；确保始终处于运行状态（符合用途）；确保有人负责并得到物理保护。还需确保对支持服务能力至关重要的资产始终可靠且可用。管理软件许可证，以确保根据所需的业务用量购置、保留和部署最合适的数量，同时安装的软件符合许可协议。

目的

核算所有 I&T 资产并优化这些资产提供的价值。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG04 财务信息的质量 • EG07 管理信息的质量 • EG09 业务流程成本的优化	AG04 技术相关财务信息的质量

企业目标的指标示例	
EG04	a. 有关企业财务信息的透明度、了解度和准确性的关键利益相关方满意度调查 b. 不遵守财务相关法规的成本
EG07	a. 董事会和执行管理层对决策信息的满意度 b. 基于不准确信息的错误业务决策所导致的事故数量 c. 为有效业务决策提供支持性信息所花的时间 d. 管理信息的及时性
EG09	a. 成本与达到的服务水平的比率 b. 董事会和执行管理层对业务流程成本的满意度

一致性目标的指标示例	
AG04	a. 有关 I&T 财务信息的透明度、了解度和准确性水平的关键利益相关方满意度 b. 已定义运营成本和预期效益并获得批准的 I&T 服务的百分比

A. 组件：流程

管理实践	指标示例
BAI09.01 识别并记录当前资产。 确保交付服务所需的所有 I&T 资产的记录保持最新且准确，并由期望未来效益（包括具有经济价值的资源，如硬件或软件）的组织拥有或控制。确保资产与配置管理和财务管理保持一致。	a. 在资产登记表中准确记录的资产的百分比 b. 符合用途的资产的百分比 c. 已清点并保持最新状态的资产的百分比

活动	能力级别
1. 确定记录当前状态的资产登记表中的所有自有资产。在资产负债表中报告资产；购买或创建资产以增加公司价值或促进企业运营（如硬件和软件）。确定所有自有资产并加以维护，使其与变更管理和配置管理流程、配置管理系统和财务会计记录保持一致。	2
2. 识别在管理资产时需要满足的法律、监管或合同要求。	
3. 验证资产是否符合用途（即处于有用状态）。	
4. 确保对所有资产进行核算。	3
5. 定期执行物理和逻辑库存检查和对帐，以验证所有自有资产的存在情况，包括使用软件发现工具进行验证。	4
6. 定期确定各项资产能否继续提供价值。如是，估算可实现价值的预计可用寿命。	

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI Cybermaturity Platform，2018 年	RI.AD Asset Discovery & Identification
ISF, The Standard of Good Practice for Information Security 2016	BA1.1 Business Application Register
ISO/IEC 27002:2013/Cor.2:2015(E)	8.1 Responsibility for assets
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.13 Physical and environmental protection (PE-9)
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 1: Inventory of Authorized and Unauthorized Devices; CSC 2: Inventory of Authorized and Unauthorized Software
管理实践	**指标示例**
BAI09.02 管理关键资产。 识别对提供服务能力至关重要的资产。最大限度提高这些资产的可靠性和可用性以支持业务需求。	a. 关键资产的数量 b. 每项关键资产的平均停机时间 c. 已识别的事故趋势数量

活动	能力级别
1. 通过参考服务定义、SLA 和配置管理系统中的要求，识别对提供服务能力至关重要的资产。	2
2. 定期考虑各项关键资产的故障风险或置换需求风险。	
3. 向受到影响的客户和用户传达维护活动的预期影响（如性能限制）。	
4. 将计划内停机时间纳入整体生产计划。安排维护活动以尽量减少对业务流程造成的不利影响。	3
5. 通过定期执行预防性维护来保持关键资产的恢复能力。监控性能并根据需要提供备用和/或额外资产，以最大限度降低发生故障的可能性。	
6. 考虑成本/效益分析、供应商建议、中断风险、合格人员和其他相关因素，为所有硬件制定预防性维护计划。	
7. 就第三方访问组织的 I&T 设施以开展现场和异地活动（如外包）建立维护协议。制定包含或提及所有必要安全和隐私条件（包括访问授权程序）的正式服务合同，以确保符合组织安全/隐私政策和标准。	
8. 确保仅在必要时激活远程访问服务和用户配置文件（或其他用于维护或诊断的方法）。	
9. 通过检查事故趋势对关键资产的性能进行监控。必要时，采取措施进行维修或更换。	4

相关指南（标准、框架、合规性要求）	**详细参考**
美国国家标准与技术研究所，Framework for Improving Critical Infrastructure Cybersecurity，第 1.1 版，2018 年 4 月	ID.AM Asset Management
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.13 Physical and environmental protection (PE-20)
管理实践	**指标示例**
BAI09.03 管理资产的生命周期。 管理资产从采购到处置的完整生命周期。确保资产在停用之前得到了尽可能有效和高效的使用、考虑以及物理保护。	a. 在从采购到处置的完整生命周期内得到妥当管理的资产的百分比 b. 每项资产的利用率 c. 在标准实施生命周期之后部署的资产的百分比

A. 组件：流程（续）	
活动	**能力级别**
1. 根据经批准的请求和企业采购政策和实践采购所有资产。	2
2. 以受控的方式采购、接收、验证、测试和记录所有资产，包括所需的物理标记。	
3. 根据商定的合同条件批准付款并与供应商完成流程。	
4. 按照标准实施生命周期部署资产，包括变更管理和验收测试。	3
5. 将资产分配给承担相关责任的用户并请其签收（如适用）。	
6. 当因为用户角色的变更、服务中的冗余或服务终止而不再需要这些资产时，应尽可能重新进行分配。	
7. 计划、授权和实施与资产停用相关的活动，保留相关记录以满足持续的业务和监管需求。	
8. 采用安全的方式处置资产，例如，考虑永久删除媒体设备记录的任何数据和处置可能对环境有害的资产时。	
9. 当因为所有相关服务终止、技术过时或缺乏用户而导致资产无实际用途时，应考虑对环境的影响，以负责任的方式处置这些资产。	4
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI Cybermaturity Platform，2018 年	DP.ML Manage Asset Lifecycle
ISF, The Standard of Good Practice for Information Security 2016	IM2.1 Document Management; PA1.1 Hardware Life Cycle Management
ITIL 第 3 版，2011 年	Service Transition, 4.3 Service Asset and Configuration Management
美国国家标准与技术研究所，Framework for Improving Critical Infrastructure Cybersecurity，第 1.1 版，2018 年 4 月	PR.MA Maintenance
管理实践	**指标示例**
BAI09.04 优化资产价值。 定期审查总体资产基础，确定以符合业务需求的方式优化价值的方法。	a. 基准成本 b. 未被利用的资产数量
活动	**能力级别**
1. 定期审查总体资产基础，考虑其是否符合业务要求。	3
2. 评估维护成本，考虑合理性，并确定成本更低的方案。必要时可用新的备用方案替代。	4
3. 审查保修条款并考虑性价比和替代策略，以确定成本最低的方案。	5
4. 使用容量和利用情况的统计信息来识别利用率低下或冗余的资产，可考虑处置或更换这些资产以降低成本。	
5. 审查总体资产基础，以识别可实施标准化、单一采购和其他可降低采购、支持和维护成本的策略的机会。	
6. 审查总体资产状态，以寻找利用新兴技术或替代采购策略的机会，从而降低成本或提高性价比。	
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	
管理实践	**指标示例**
BAI09.05 管理许可证。 管理软件许可证以维护最佳数量的许可证并为业务需求提供支持。确保拥有的许可证数量足以覆盖正在使用的已安装软件。	a. 已使用许可证相对已购买许可证的比率 b. 仍在付款但尚未使用的许可证的百分比 c. 应进行升级以实现更高价值的产品和许可证的百分比

A. 组件：流程（续）	
活动	**能力级别**
1. 维护一份包含所有已购买软件许可证和相关许可协议的登记表。	2
2. 定期进行审计，以识别所有已安装的许可软件实例。	3
3. 将已安装的软件实例数量与拥有的许可证数量进行比较。确保许可证的合规性衡量方法符合许可证和合同要求。	4
4. 当实例低于所拥有的数量时，考虑能否节省非必要的维护、培训和其他成本，从而决定是否需要保留或终止许可。	
5. 当实例数高于拥有的数量时，首先考虑能否卸载不再需要或不再合理的实例，然后考虑在必要的情况下购买额外的许可证以遵守许可协议。	
6. 定期考察升级产品和相关的许可证能否实现更多价值。	5

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构										
关键管理实践	**首席信息官**	**首席技术官**	**架构总监**	**开发总监**	**IT 运营总监**	**IT 行政总监**	**服务经理**	**信息安全经理**	**隐私官**
BAI09.01 识别并记录当前资产。		A			R	R			
BAI09.02 管理关键资产。		A	R	R	R	R		R	R
BAI09.03 管理资产的生命周期。		A			R	R	R		
BAI09.04 优化资产价值。	A	R	R	R	R	R	R		
BAI09.05 管理许可证。	A	R		R	R	R			

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
BAI09.01 识别并记录当前资产。	自	描述	描述	至
	BAI03.04	资产清单的更新	预期用途审查的结果	APO02.02
	BAI10.02	配置贮存库	资产登记表	APO06.01；BAI10.03
			实际库存检查的结果	BAI10.03；BAI10.04；DSS05.03
BAI09.02 管理关键资产。			关于计划内维护停机时间的沟通	APO08.04
			维护协议	内部
BAI09.03 管理资产的生命周期。			已授权的资产停用	BAI10.03
			更新的资产登记表	BAI10.03
			经批准的资产采购请求	内部
BAI09.04 优化资产价值。			降低资产成本或提升价值的机会	APO02.02
			成本优化审查的结果	APO02.02
BAI09.05 管理许可证。			调整许可证数量和分配情况的行动计划	APO02.05
			软件许可证登记表	BAI10.02
			已安装许可证的审计结果	MEA03.03
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
资产管理	Skills Framework for the Information Age，第 6 版，2015 年	ASMG
系统安装/弃用	Skills Framework for the Information Age，第 6 版，2015 年	HSIN

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
资产管理政策	提供资产生命周期管理、资产保护措施、系统分类和所有权、数据所有权和数据分类的相关准则		
知识产权 (IP) 政策	解决与员工 I&T 相关的创造性工作输出（如软件开发）的使用、所有权、销售和分发有关的风险。要求从工作开始时便维护相应的文档、详细程度等。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
建立以开放、一致且透明的方式识别、评估和向企业报告各项资产的相对经济和战略价值的文化。		

G. 组件：服务、基础设施和应用程序
资产管理工具

领域：内部构建、外部采购和实施 管理目标：BAI10 — 妥当管理的配置	焦点领域：COBIT 核心模型

描述

定义和维护就提供 I&T 促成的服务所需的关键资源和能力的描述和关系，包括收集配置信息、建立基准、验证和审核配置信息以及更新配置贮存库。

目的

提供关于服务资产的充分信息，以有效地管理服务。评估变更影响并处理服务事故。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG02 妥当管理的业务风险 • EG06 业务服务连续性和可用性	AG07 信息、参与执行的基础设施和应用程序的安全，以及隐私的安全
企业目标的指标示例	**一致性目标的指标示例**
EG02 a. 风险评估涵盖的关键业务目标和服务的百分比 b. 风险评估未发现的重大事故数量与总事故数量的比率 c. 风险概况的更新频率	AG07 a. 导致财务损失、业务中断或公众形象受损的保密性事故的数量 b. 导致财务损失、业务中断或公众形象受损的可用性事故的数量 c. 导致财务损失、业务中断或公众形象受损的完整性事故的数量
EG06 a. 导致重大事故的客户服务或业务流程中断的次数 b. 事故的业务成本 c. 因计划外服务中断而损失的业务处理小时数 d. 与承诺的服务可用性目标有关的投诉百分比	

A. 组件：流程

管理实践	指标示例
BAI10.01 建立和维护配置模型。 建立和维护有关服务、资产和基础设施以及配置项 (CI) 记录及其之间的关系的逻辑模型，包括有效管理服务所需的 CI，为服务中的各个资产提供单一可靠的描述。	a. 签字批准配置模型的利益相关方的数量 b. 配置项关系保持准确的百分比

活动	能力级别
1. 定义和商定配置管理的范围和详细程度（即要包括哪些服务、资产和基础设施可配置项）。	3
2. 建立和维护配置管理的逻辑模型，包括 CI 类型、属性、关系类型、关系属性和状态代码的相关信息。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Supporting Processes - Configuration Management
ISF, The Standard of Good Practice for Information Security 2016	SY1 System Configuration
ISO/IEC 20000-1:2011(E)	9.1 Configuration management
ITIL 第 3 版，2011 年	Service Transition, 4.3 Service Asset and Configuration Management
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.5 Configuration management (CM-6)

A. 组件：流程（续）	
管理实践	**指标示例**
BAI10.02 建立和维护配置贮存库和基准。 建立和维护配置管理贮存库并创建受控的配置基准。	a. 贮存库中列出的配置项 (CI) 数量 b. 服务、应用程序或基础设施的配置基准保持准确的百分比
活动	**能力级别**
1. 识别 CI、对其进行分类，并填充贮存库。	2
2. 创建、审查并正式商定服务、应用程序或基础设施的配置基准。	3
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI Cybermaturity Platform，2018 年	IP.CB Apply Configuration Baselines
美国国家标准与技术研究所特别出版物 800-37， 修订版 2（草稿），2018 年 5 月	3.4 Implementation (Task 2)
美国国家标准与技术研究所特别出版物 800-53， 修订版 5（草稿），2017 年 8 月	3.19 System and service acquisition (SA-10)
管理实践	**指标示例**
BAI10.03 维护和控制配置项。 通过填充任何配置变更来维护最新的配置项 (CI) 贮存库。	a. 贮存库的变更/更新频率 b. CI 贮存库保持准确和完整的百分比
活动	**能力级别**
1. 定期确定所有 CI 变更。	2
2. 为确保完整性和准确性，对照基准审查建议的 CI 变更。	
3. 更新经批准的 CI 变更的配置详细信息。	
4. 创建、审查并正式商定配置基准变更（如需要）。	3
相关指南（标准、框架、合规性要求）	**详细参考**
美国国家标准与技术研究所特别出版物 800-53， 修订版 5（草稿），2017 年 8 月	3.5 Configuration management (CM-2)
管理实践	**指标示例**
BAI10.04 生成状态和配置报告。 定义并生成关于配置项状态变更的配置报告。	a. 已识别的未授权变更的数量 b. CI 的状态变更相对基准保持准确的百分比
活动	**能力级别**
1. 根据基准识别 CI 的状态变更并进行报告。	2
2. 将所有配置变更与经批准的变更请求进行匹配，以识别任何未经授权的变更。向变更管理团队报告未经授权的变更。	3
3. 确定所有利益相关方的报告要求，包括内容、频率和介质。根据确定的要求生成报告。	
相关指南（标准、框架、合规性要求）	**详细参考**
美国国家标准与技术研究所特别出版物 800-53， 修订版 5（草稿），2017 年 8 月	3.5 Configuration management (CM-3)
管理实践	**指标示例**
BAI10.05 验证并审查配置贮存库的完整性。 定期审查配置贮存库并对照期望的目标验证完整性和正确性。	a. 配置贮存库与在用配置之间的偏差数量 b. 与配置信息不完整或缺失有关的偏差数量

A. 组件：流程（续）	
活动	**能力级别**
1. 通过比较物理和逻辑配置以及使用适当的发现工具（如需要），定期对照配置贮存库验证在用配置项。	4
2. 报告并审查所有偏差，以期获得批准，采取纠正措施，或移除任何未经授权的资产。	
3. 定期验证贮存库中定义的所有物理配置项是否实际存在。向管理层报告任何偏差。	
4. 根据业务需求设定配置贮存库的完整性目标并定期进行审查。	
5. 定期对照目标比较完整度和准确度，并根据需要采取补救措施，以提高贮存库的数据质量。	5

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.5 Configuration management (CM-4)

B. 组件：组织结构								
关键管理实践	**首席信息官**	**首席技术官**	**架构总监**	**开发总监**	**IT 运营总监**	**IT 行政总监**	**服务经理**	**信息安全经理**
BAI10.01 建立和维护配置模型。		A			R	R	R	
BAI10.02 建立和维护配置贮存库和基准。		A		R	R	R	R	R
BAI10.03 维护和控制配置项。	A	R		R	R	R		
BAI10.04 生成状态和配置报告。		A			R	R		
BAI10.05 验证并审查配置贮存库的完整性。		A	R	R	R		R	

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
BAI10.01 建立和维护配置模型。	自	描述	描述	至
	BAI07.06	发布计划	逻辑配置模型	内部
			配置管理模型的范围	内部
BAI10.02 建立和维护配置贮存库和基准。	BAI09.05	软件许可证登记表	配置基准指标	BAI03.11；BAI03.12
			配置贮存库	BAI09.01；DSS02.01
BAI10.03 维护和控制配置项。	BAI06.03	变更请求状态报告	经批准的基准变更	BAI03.11
	BAI09.01	• 资产登记表 • 物理库存检查的结果	更新的配置项贮存库	DSS02.01
	BAI09.03	• 更新的资产登记表 • 已授权的资产停用		
BAI10.04 生成状态和配置报告。	BAI09.01	实际库存检查的结果	配置状态报告	BAI03.11；DSS02.01
BAI10.05 验证并审查配置贮存库的完整性。			贮存库完整性审查的结果	内部
			配置项物理验证的结果	内部
			许可证偏差	MEA03.03

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-37，修订版 2，2017 年 9 月	3.4 Implementation (Task 2): Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
配置管理	Skills Framework for the Information Age，第 6 版，2015 年	CFMG

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
配置管理政策	传达建立和使用综合配置贮存库的相关指南，包括所有技术组件、相关的配置定义以及与其他技术组件的相互依存关系。帮助确保最大限度降低系统和软件变更对服务造成的破坏。确保变更在适用的群组之间协调一致，不会引起相互冲突或重复的工作。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
建立支持跨部门的结构化配置管理方法的文化，让用户认识到严格的配置管理的价值（如避免版本冲突或重复的工作）并应用妥善实施的规则和程序。		

G. 组件：服务、基础设施和应用程序
配置管理工具和贮存库

领域：内部构建、外部采购和实施 管理目标：BAI11 — 妥当管理的项目	焦点领域：COBIT 核心模型

描述

根据标准项目管理方法，以协调一致的方式管理企业内部发起的所有符合企业战略的项目。启动、计划、控制和执行项目，并在完成实施后审查之后将其关闭。

目的

通过改进与业务部门和最终用户的沟通并提高他们的参与度来实现定义的项目成果，并降低因意外的延迟、成本和价值流失带来的风险。确保项目交付成果的价值和质量，并最大程度地提高它们对定义的计划和投资组合的贡献。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	• AG03 通过 I&T 促成的投资和服务组合所实现的效益 • AG06 将业务需求转化为可运作的解决方案的敏捷性 • AG09 在预算内按时交付计划且满足要求和质量标准
企业目标的指标示例	**一致性目标的指标示例**
EG01 a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG03 a. 达到或超过业务案例宣称效益的 I&T 促成的投资的百分比 b. 实现预期效益（如服务水平协议所述）的 I&T 服务的百分比
EG08 a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度	AG06 a. 业务高管对 I&T 响应新需求的满意度水平 b. 新的 I&T 相关服务和应用程序的平均上市时间 c. 将战略 I&T 目标转化为议定的已批准举措所需的平均时间 d. 受最新基础设施和应用支持的关键业务流程的数量
EG12 a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比	AG09 a. 在预算内按时交付的计划/项目的数量 b. 因质量缺陷需要重大返工的计划的数量 c. 对计划/项目质量满意的利益相关方的百分比

A. 组件：流程	
管理实践	**指标示例**
BAI11.01 维护标准的项目管理方法。 维护标准的项目管理方法，以便开展治理和管理审查、决策制订和交付管理活动。这些活动应始终关注业务价值和目标（即需求、风险、成本、日程表和质量目标）。	a. 根据既定的标准方法取得成功的项目百分比 b. 项目管理方法、良好实践、工具和模板的更新次数

活动	能力级别
1. 维护和实施标准的项目管理方法，确保该方法与企业的特定环境保持一致，并运用基于既定流程和相应技术的良好实践。确保该方法涵盖整个生命周期和需要遵循的科目，包括范围、资源、风险、成本、质量、时间、沟通、利益相关方参与、采购、变更控制、整合和效益实现的管理。	2
2. 提供适当的项目管理培训，并考虑让项目经理获取认证。	
3. 设立项目管理办公室 (PMO)，负责在整个组织范围内维护标准的计划和项目管理方法。PMO 通过创建和维护需要的项目文档模板，为项目经理提供培训和最佳实践，跟踪项目管理所用最佳实践的相关指标等方式，为所有项目提供支持。在某些情况下，PMO 还会向高级管理层和/或利益相关方报告项目进展情况，帮忙排定项目优先级，并确保所有项目都能支持企业的总体业务目标。	3
4. 评估在使用项目管理方法时吸取的经验教训。相应地更新良好实践、工具和模板。	4

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.15 Program management (PM-2)

管理实践	指标示例
BAI11.02 制定并启动项目。 定义并记录项目的性质和范围，确保利益相关方对项目范围达成共识。定义应得到项目发起人的正式批准。	a. 批准企业需求、范围、计划内成果和项目风险水平的利益相关方的百分比 b. 利益相关方收到明确定义项目性质、范围和效益的书面声明的项目百分比

活动	能力级别
1. 为推动利益相关方对项目范围达成共识，应为他们提供明确定义每个项目的性质、范围和交付成果的书面声明。	2
2. 确保每个项目都有一个或多个具有足够权限的发起人，以管理整个计划中的项目运行。	
3. 确保企业内的关键利益相关方和发起人（业务和 IT 部门）同意并接受项目要求，包括项目成功（验收）标准和关键绩效指标 (KPI) 的定义。	
4. 指定一名专门负责项目的经理。确保其具备必要的技术和业务知识以及相应的胜任能力和技能，能够有效和高效地管理项目。	
5. 确保项目定义描述了项目沟通计划的要求，该计划确定了内部和外部的项目沟通。	
6. 获得利益相关方的批准后，在整个项目期间维护项目定义，以反映不断变化的需求。	
7. 为跟踪项目的执行情况，应建立可及时执行的跟踪机制，例如定期报告和阶段-关卡、发布或阶段审查，并获得相应的批准。	

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 4.1 Develop project charter; Part 1: 6. Project schedule management

A. 组件：流程（续）	
管理实践	**指标示例**
BAI11.03 管理利益相关方的参与。 管理利益相关方参与，确保积极地与所有相关的利益相关方交换准确、一致且及时的信息。这包括制定计划、识别利益相关方、推动他们参与并管理他们的期望。	a. 利益相关方对参与度的满意程度 b. 有效参与的利益相关方的百分比
活动	**能力级别**
1. 计划如何在项目的整个生命周期内识别、分析、联络和管理企业内外部的利益相关方。	3
2. 通过建立和维护适当级别的协调、沟通和联络来识别、联系和管理利益相关方，确保他们参与该项目。	
3. 分析利益相关方的利益、需求和参与度。必要时采取补救行动。	4
相关指南（标准、框架、合规性要求）	**详细参考**
PMBOK Guide，第 6 版，2017 年	Part 1: 13. Project stakeholder management Part 1: 10. Project communications management
管理实践	**指标示例**
BAI11.04 制定和维护项目计划。 建立并维护正式、获得批准的项目整合计划（涵盖业务和 IT 资源），以指导整个项目期间的项目执行和控制。应明确定义项目范围并关联到建立或增强业务能力。	a. 在缺少有效的、更新的项目价值地图的情况下实施进行中的项目的百分比 b. 已完成计划中的里程碑或任务的百分比
活动	**能力级别**
1. 开发项目计划来提供信息，使管理层能够逐步控制项目进度。该计划应包括以下详细信息：项目交付成果和验收标准；所需的内部和外部资源和职责；明确的工作分解结构和工作包；所需资源的估算；里程碑/发布计划/阶段；关键依赖关系；预算和成本；以及对关键路径的识别。	2
2. 维护项目计划和任何依存计划（例如风险计划、质量计划、效益实现计划）。确保这些计划保持最新并反映了实际进度和获得对重大变更的批准。	
3. 确保项目计划和进度报告得到有效的沟通。确保对个别计划所做的任何变更都会反映到其它计划中。	
4. 确定项目内以及计划内多个项目之间的活动、相互依赖关系以及所需的协作和沟通。	
5. 确保每个里程碑都有需要审查和签字批准的重要交付成果。	
6. 建立项目基准指标（例如成本、日程表、范围、质量）且经过适当的审查、批准及纳入整合的项目计划中。	
相关指南（标准、框架、合规性要求）	**详细参考**
PMBOK Guide，第 6 版，2017 年	Part 1: 4.2 Develop project management plan
管理实践	**指标示例**
BAI11.05 管理项目质量。 制定和执行符合质量管理标准 (QMS) 的质量管理计划、流程和实践。描述项目质量方法及其实施。应由所有相关方正式审批计划并达成共识，并将其纳入整合的项目计划中。	a. 零错误产品构建的百分比 b. 取消的项目的数量

A. 组件：流程（续）	
活动	**能力级别**
1. 为保证项目交付成果的质量，应确定所有权和责任、质量审查流程、成功标准和绩效指标。	2
2. 确定在项目规划期间为新系统或改进的系统提供认证支持所需的鉴证任务和实践。将它们纳入到整合的计划中。确保这些任务能够保证内部控制以及安全和隐私解决方案满足定义的要求。	3
3. 定义对计划中的可交付成果质量进行独立验证和校验的任何要求。	
4. 根据质量管理计划和质量管理体系 (QMS) 执行质量保证和控制活动。	

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 8. Project quality management

管理实践	指标示例
BAI11.06 管理项目风险。 通过系统性的流程（包括规划、识别、分析、应对和监控潜在导致预期外的变更的领域或事件）来消除或最大程度地减少与项目相关的特定风险。定义和记录项目管理面临的任何风险。	a. 已识别的延迟和问题的数量 b. 采用与 ERM 框架一致的正式项目风险管理方法的项目数量

活动	能力级别
1. 制定与 ERM 框架一致的正式项目风险管理方法。确保该方法包括风险识别、分析、应对、缓解、监控和控制。	2
2. 为具备相应技能的人员分配执行项目内的企业项目风险管理流程的职责，并确保将此纳入解决方案开发实践中。考虑将此角色分配给独立团队，尤其是客观视点被需要或该项目计划被视为关键时。	
3. 确定规避、接受或缓解风险的行动的所有者。	
4. 执行项目风险评估，在整个项目中持续识别和量化风险。在项目治理结构中恰当地管理和沟通风险。	3
5. 定期重新评估项目风险，包括启动每个主要项目阶段时，以及评估重大变更请求时。	
6. 维护和审查包含所有潜在项目风险的风险登记表，以及包含所有项目问题及其解决方案的风险缓解日志。定期分析日志中的趋势和反复发生的问题，确保根本原因得到纠正。	

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.15 Program management (PM-4)
PMBOK Guide，第 6 版，2017 年	Part 1: 11. Project risk management

管理实践	指标示例
BAI11.07 监控项目。 对照关键项目绩效衡量标准（例如进度、质量、成本和风险）衡量项目绩效。识别任何偏离预期目标的情况。评估偏离期望的情况对项目和整体计划的影响，并将结果报告给关键利益相关方。	a. 与范围和预期成果保持一致的活动的百分比 b. 已解决的偏离计划情况的百分比 c. 项目状态审查的频次

A. 组件：流程（续）	
活动	**能力级别**
1. 建立并使用一系列项目标准，包括但不限于范围、预期业务效益、进度、质量、成本和风险水平。	2
2. 向已确定的关键利益相关方报告项目进度、与既定的关键项目绩效标准（包括但不限于预期业务效益）的偏差，以及可能对项目产生的积极和消极影响。	
3. 记录任何必要的变更并提交给项目的关键利益相关方，获得他们的批准之后再采用。与项目经理沟通修订之后的标准，用于未来的绩效报告。	
4. 对于每个迭代周期、版本或项目阶段生成的交付成果，应获得受影响的业务和 IT 职能部门中指定的经理和用户的批准和签字确认。	
5. 在开始项目阶段或迭代交付成果的工作之前，根据关键利益相关方议定的明确定义的验收标准制定审批流程。	3
6. 在议定的主要阶段-关卡、发布或迭代周期评估项目。根据预定的关键成功标准作出继续/停止的正式决定。	
7. 建立并运行项目的变更控制系统，以便对项目基准指标（例如范围、预期业务收益、进度、质量、成本、风险等级）的所有变更进行适当的审查、批准并纳入整合的项目计划中，使其与计划和项目治理框架保持一致。	
8. 根据关键项目绩效标准衡量项目绩效。分析与既定的关键项目绩效标准发生偏差的原因，并评估可能对项目产生的积极和消极影响。	4
9. 监控项目的变更并审查现有的关键项目绩效标准，以确定这些标准是否仍能有效地衡量进度。	
10. 必要时，根据项目治理框架提出并监控补救行动。	
相关指南（标准、框架、合规性要求）	**详细参考**
PMBOK Guide，第 6 版，2017 年	Part 1: 4.5 Monitor and control project work
管理实践	**指标示例**
BAI11.08 管理项目资源和工作包。 通过对授权和接受工作包提出正式要求，并分配和协调适当的业务和 IT 资源，来管理项目工作包。	a. 资源问题（如技能、容量）的数量 b. 为项目经理、分配的员工以及其他相关方明确定义的角色、职责和管理特权的数量
活动	**能力级别**
1. 识别项目的业务和 IT 资源需求，并明确匹配适当的角色和职责，同时对上报和决策权达成共识并充分理解。	2
2. 识别项目阶段里定义的相关角色所涉及的所有人员应满足的技能和时间要求。根据可用的技能信息（例如 IT 技能矩阵）分配角色。	
3. 利用经验丰富的项目管理和团队领导资源（这些资源所具备的技能足以应对项目的规模、复杂度和风险）。	
4. 考虑并明确定义其它相关方的角色和职责，包括财务、法务、采购、人力资源、内部审计以及合规方面。	
5. 明确定义和议定第三方产品和服务的采购和管理责任并管理这些关系。	
6. 根据项目计划识别并授权执行工作。	
7. 识别项目计划差距并向项目经理提出反馈以进行补救。	
相关指南（标准、框架、合规性要求）	**详细参考**
PMBOK Guide，第 6 版，2017 年	Part 1: 4.3 Direct and manage project work

A. 组件：流程（续）	
管理实践	**指标示例**
BAI11.09 关闭项目或迭代。 在每个项目、发布或迭代结束时，需要项目的利益相关方确定该项目、发布或迭代是否实现了所需的能力成果，并像预期那样推动计划效益的实现。识别和沟通任何未完成的活动，以实现项目计划的成果和/或计划的效益。识别和记录经验教训，以便用于未来的项目、发布、迭代和计划。	a. 在项目收尾审查时利益相关方表示的满意度水平 b. 第一次就通过验收成果的百分比

活动	能力级别
1. 使利益相关方接受项目交付成果并移交所有权。	2
2. 定义并应用关键的项目收尾步骤，包括评估项目是否取得预期结果的实施后审查。	3
3. 计划并执行实施后审查，以确定项目是否取得预期结果。改进项目管理和系统开发过程方法论。	
4. 识别、分配、沟通和跟踪任何未完成的活动，以确保项目取得了需要的能力成果，并对计划效益的实现做出了预期的贡献。	
5. 定期以及在项目结束后向项目参与者收集经验教训。审查这些经验教训以及创造效益和价值的关键活动。分析数据并提出建议，以改进当前项目以及未来项目的项目管理方法。	4

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 4.7 Close project or phase

B. 组件：组织结构												
关键管理实践	**首席执行官**	**首席风险官**	**首席信息官**	**首席技术官**	**业务流程所有者**	**（计划/项目）指导委员会**	**计划经理**	**项目经理**	**项目管理办公室**	**开发总监**	**信息安全经理**
BAI11.01 维护标准的项目管理方法。	A		R				R	R			
BAI11.02 制定并启动项目。		R		R	R	A	R	R	R	R	
BAI11.03 管理利益相关方的参与。			R			A		R			
BAI11.04 制定和维护项目计划。						A		R	R		
BAI11.05 管理项目质量。		R	R			A		R			R
BAI11.06 管理项目风险。			R			A		R			R
BAI11.07 监控项目。					R	A		R	R	R	
BAI11.08 管理项目资源和工作包。					R	A	R		R	R	
BAI11.09 关闭项目或迭代。						A		R	R		

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 3. The role of the project manager

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
BAI11.01 维护标准的项目管理方法。	APO03.04	• 架构治理需求 • 实施阶段描述	更新的项目管理方法	内部
	APO10.04	已识别的供应商交付风险		
	EDM02.03	阶段-关卡审查的需求		
	EDM02.04	改进实现价值的措施		
BAI11.02 制定并启动项目。			项目定义	内部
			项目范围声明	内部
BAI11.03 管理利益相关方的参与。			利益相关方参与的有效性评估结果	内部
			利益相关方参与计划	内部
BAI11.04 制定和维护项目计划。	BAI07.03	已批准的验收测试计划	项目报告和沟通	内部
			项目基准指标	内部
			项目计划	内部
BAI11.05 管理项目质量。	APO11.01	质量管理计划	项目质量管理计划	BAI02.04; BAI03.06; BAI07.01
	APO11.02	客户对质量管理的要求	项目交付成果的独立验证要求	BAI07.03
BAI11.06 管理项目风险。	APO12.02	风险分析结果	项目风险登记表	内部
	BAI02.03	• 需求风险登记表 • 风险缓解措施	项目风险评估结果	内部
	在 COBIT 外部	企业风险管理 (ERM) 框架	项目风险管理计划	内部
BAI11.07 监控项目。			议定的项目变更	内部
			项目进度报告	内部
			项目绩效标准	内部
BAI11.08 管理项目资源和工作包。			项目资源要求	APO07.05; APO07.06
			项目规划中的缺口	内部
			项目角色和职责	内部

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
BAI11.09 关闭项目或迭代。	**自**	**描述**	**描述**	**至**
	BAI07.08	• 实施后审查报告 • 补救行动计划	实施后审查结果	APO02.04
			利益相关方的项目验收确认	内部
			吸取的项目经验教训	内部

相关指南（标准、框架、合规性要求）	详细参考
PMBOK Guide，第 6 版，2017 年	Part 1: 4. Project integration management: Inputs and Outputs; Part 1: 6. Project schedule management: Inputs and Outputs; Part 1: 10. Project communications management: Inputs & Outputs; Part 1: 11. Project risk management: Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
组合、计划和项目支持	Skills Framework for the Information Age，第 6 版，2015 年	PROF
项目和组合管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage—E.2. Project and Portfolio Management
项目管理	Skills Framework for the Information Age，第 6 版，2015 年	PRMG

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
计划/项目管理政策	指导与计划和项目有关的风险管理。详细说明关于计划和项目管理的管理职位和期望。在计划/项目执行期间处理有关绩效、预算、风险分析、不良事件的报告和缓解的问责、目的和目标。	PMBOK Guide，第 6 版，2017 年	Part 1: 2.3.1 Processes, policies and procedures

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
考虑组织结构和业务环境，建立企业范围的项目管理文化，确保在整个企业内以一致和最佳的方式实施项目管理。确保将所有举措转换为项目（或范围较小的变更）；确保不会发生超出项目管理范围的临时行动。		

G. 组件：服务、基础设施和应用程序
项目管理工具

4.4 交付、服务和支持 (DSS)

01 妥当管理的运营

02 妥当管理的服务请求和事故

03 妥当管理的问题

04 妥当管理的连续性

05 妥当管理的安全服务

06 妥当管理的业务流程控制

领域：交付、服务与支持 管理目标：DSS01 — 妥当管理的运营	焦点领域：COBIT 核心模型

描述

协调和执行必要的活动和运营程序来提供内部和外包 I&T 服务，包括执行预先定义的标准操作规程和必要的监控活动。

目的

按计划提供可运行的 I&T 产品和服务成果。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化	AG05 提供符合业务需求的 I&T 服务
企业目标的指标示例	**一致性目标的指标示例**
EG01 a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG05 a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG08 a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度	

A. 组件：流程

管理实践	指标示例
DSS01.01 执行运营程序。 可靠而一致地维护和执行运营程序和运营任务。	a. 由运营问题导致的事故的数量 b. 已执行的非标准操作规程的数量

活动	能力级别
1. 制定并维护操作规程和相关活动，以支持交付的所有服务。	2
2. 维护运营活动时间表并开展活动。	
3. 确认是否已接收预期要处理的所有数据并已完整、准确和及时地进行处理。交付满足企业要求的输出内容。支持重新开始和重新处理的需求。确保用户以安全的方式及时接收正确的输出内容。	3
4. 管理已安排活动的绩效和吞吐量。	4
5. 监控与运营程序有关的事故和问题，并采取适当措施提高已执行的运营任务的可靠性。	5

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	TP.SE Safeguard Operational Environment
HITRUST CSF，第 9 版，2017 年 9 月	09.01 Document Operating Procedures
ISO/IEC 27002:2013/Cor.2:2015(E)	12.1 Operational procedures and responsibilities
ITIL 第 3 版，2011 年	Service Operation, 4.1 Event Management
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.13 Physical and environmental protection (PE-13, PE-14, PE-15)

A. 组件：流程（续）	
管理实践	**指标示例**
DSS01.02 管理外包的 I&T 服务。 管理外包 I&T 服务的运营，以持续保护企业信息和服务交付的可靠性。	a. 纳入外包合同中的特定/SMART KPI 的数量 b. 外包合作伙伴未能达到 KPI 的频次

活动	能力级别
1. 确保企业对信息安全流程的要求与托管或提供服务的第三方的合同和 SLA 相契合。	3
2. 确保企业的运营业务和 IT 处理要求以及服务交付的优先级与托管或提供服务的第三方的合同和 SLA 相契合。	
3. 整合关键的内部 IT 管理流程与那些外包服务提供商的流程。这些流程应包括，例如：性能和容量规划、变更管理、配置管理、服务请求和事故管理、问题管理、安全管理、业务连续性，以及流程绩效监控和报告。	
4. 制定对外包提供商的运营环境进行独立审计和鉴证的计划，以确保提供商充分满足议定的要求。	4

相关指南（标准、框架、合规性要求）	详细参考
ISF, The Standard of Good Practice for Information Security 2016	SC1.2 Outsourcing
ISO/IEC 20000-1:2011(E)	4.2 Governance of processes operated by other parties

管理实践	指标示例
DSS01.03 监控 I&T 基础设施。 监控 I&T 基础设施和相关的事件。在运营日志中存储足够的时间顺序信息，以重建和审查运营及运营相关活动或支持性活动的时间顺序。	a. 自动检测系统涵盖到的关键运营事件类型的百分比 b. 根据服务关键性及配置项 (CI) 与依赖 CI 的服务之间的关系进行监控的基础设施资产的百分比

活动	能力级别
1. 记录事件。基于对风险和绩效的考虑，确定要记录的信息级别。	2
2. 根据服务关键性以及配置项 (CI) 与依赖 CI 的服务之间的关系，确定并维护需要监控的基础设施资产列表。	3
3. 定义并实施规则，以识别和记录阈值违规和事件条件。在造成假象的轻微事件和重大事件之间找到平衡，避免事件日志因不必要的信息而过载。	
4. 生成事件日志并适当保留一段时间，以协助未来的调查。	
5. 确保在识别到与规定阈值的偏差时及时创建事故单。	
6. 建立监控时间日志的程序。执行定期审查。	4

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-53， 修订版 5（草稿），2017 年 8 月	3.10 Maintenance (MA-2, MA-3)

管理实践	指标示例
DSS01.04 管理环境。 维护用于防范环境影响因素的衡量指标。安装专业化的设备和装置来监控环境状况。	a. 接受过环境警报程序培训的人员的数量 b. 针对环境威胁定义的风险场景的数量

A. 组件：流程（续）	
活动	**能力级别**
1. 识别 IT 设施所在区域可能发生的自然的和人为灾难。评估对 IT 设施的潜在影响。	2
2. 确定如何保护 I&T 设备（包括移动和异地设备）免受环境威胁。确保相关政策限制或禁止在敏感区域饮食和吸烟，并禁止在计算机机房内存储可能造成火灾危险的办公用品和其它用品。	
3. 使 IT 站点和服务器机房始终保持清洁和安全（即干净整洁，没有纸张或纸板箱，垃圾桶没有溢出，没有易燃化学品或材料）。	
4. 确保 IT 设施的位置和构造能够最大限度降低其对环境威胁（例如盗窃、空气、火灾、烟雾、水、振动、恐怖活动、故意破坏、化学品、爆炸物）的敏感性。考虑特定的安全区域和/或防火室（例如分开存放生产和开发环境/服务器）。	3
5. 将措施和应急计划与保险要求和报告结果进行比较。及时解决不合规之处。	
6. 响应环境警报和其他通知。记录和测试程序，包括警报的优先级以及与当地应急响应机构的联系。为员工提供对这些程序的培训。	
7. 定期监控和维护主动检测环境威胁（例如，火灾、水、烟雾、湿度）的设备。	4
相关指南（标准、框架、合规性要求）	**详细参考**
美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	2.1 System and system elements; 3.2 Categorization (Task 5, 6)
管理实践	**指标示例**
DSS01.05 管理设施。 根据法律和监管要求、技术和业务要求、供应商规范以及健康和安全指导原则来管理设施，包括电力和通信设备。	a. 距离上次不间断电源测试的时间 b. 接受过健康和安全指导培训的员工的数量
活动	**能力级别**
1. 结合其它业务连续性计划需求，检查 IT 设施在预防电源波动和断电方面的要求。采购合适的不间断供电设备（例如电池、发电机），以支持业务连续性计划。	2
2. 定期测试不间断电源的机制。确保切换电源时不会对业务运营造成任何重大影响。	
3. 确保容纳 I&T 系统的设施拥有多个公用事业源（例如电力、电信、水、天然气）。分开每个设施的物理入口。	
4. 确认 IT 站点外部的电缆埋在地下或具有适当的替代保护装置。确定 IT 站点内的电缆包含在固定导管内，并且只有经过授权的人员才能进入配线柜。妥善保护电缆，使其免受火灾、烟雾、水、截取和干扰造成的损坏。	
5. 确保布线和物理修补（数据和电话）井然有序。应记录电缆和导管结构（例如蓝图、建筑物平面图和接线图）。	
6. 定期为员工提供有关健康和安全法律、法规和相关准则的培训。开展消防演练和救援演练，确保员工在发生火灾或类似事故时能够运用知识并采取行动。	
7. 确保根据供应商建议的维护间隔和规范维护 IT 站点和设备。确保仅由经过授权的人员进行维护。	3
8. 分析存放高可用性系统的设施是否满足冗余和故障切换布线要求（外部和内部）。	
9. 确保 IT 站点和设施始终满足相关的健康和安全法律、法规和准则的要求以及供应商规范。	
10. 根据 I&T 事故管理流程记录、监控、管理和解决设施事故。提供关于法律和法规要求披露的设施事故的报告。	4
11. 分析 IT 站点或场所的物理改变，以重新评估环境风险（例如火灾或水损）。向业务连续性和设施管理人员报告该分析结果。	
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	

B. 组件：组织结构							
关键管理实践	首席运营官	首席信息官	首席技术官	IT 运营总监	信息安全经理	隐私官
DSS01.01 执行运营程序。	R	A	R	R		
DSS01.02 管理外包的 I&T 服务。		A	R	R	R	R
DSS01.03 监控 I&T 基础设施。		R	A	R	R	
DSS01.04 管理环境。		R	A	R	R	
DSS01.05 管理设施。		R	A	R	R	

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
DSS01.01 执行运营程序。	BAI05.05	操作和使用计划	备份日志	内部
			运营计划表	内部
DSS01.02 管理外包的 I&T 服务。	APO09.03	• SLA • OLA	独立鉴证计划	MEA04.02
	BAI05.05	操作和使用计划		
DSS01.03 监控 I&T 基础设施。	BAI03.11	服务定义	资产监控规则和事件条件	DSS02.01；DSS02.02
			事故单	DSS02.02
			事件日志	内部
DSS01.04 管理环境。			环境政策	APO01.09
			保单报告	MEA03.03
DSS01.05 管理设施。			健康和安全意识	内部
			设施评估报告	MEA01.03

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-37，修订版 2，2017 年 9 月	3.2 Categorization (Task 5, 6): Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
数据库管理	Skills Framework for the Information Age，第 6 版，2015 年	DBAD
设施管理	Skills Framework for the Information Age，第 6 版，2015 年	DCMA
IT 基础设施	Skills Framework for the Information Age，第 6 版，2015 年	ITOP
方法和工具	Skills Framework for the Information Age，第 6 版，2015 年	METL
服务交付	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	C. Run—C.3. Service Delivery
存储管理	Skills Framework for the Information Age，第 6 版，2015 年	STMG

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
服务管理政策	提供指导和指南，确保在绩效衡量框架内有效管理和实施所有 I&T 服务，以满足业务和客户需求。涵盖 I&T 服务相关风险的管理。（ITIL 第 3 版的框架提供了关于服务管理和服务相关风险优化的详细指南。）	(1) ISO/IEC 20000-1:2011(E)；(2) ITIL 第 3 版，2011 年	(1) 4.1.2 Service management policy; (2) Service Strategy, 3. Service strategy principles

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
在整个组织内营造追求卓越的文化。鼓励员工脱颖而出。营造一个适当的环境，其中运营程序可提供必要（或更多）的服务，同时鼓励员工挑战现状和尝试新想法。通过提高员工参与度和持续改进实现卓越运营。采用以客户为中心的方法（同时包括内外部客户）。		

G. 组件：服务、基础设施和应用程序
• 云托管服务 • 基础设施监控工具 • 服务水平监控工具

本页为空白页

领域：交付、服务与支持 管理目标：DSS02 — 妥当管理的服务请求和事故	焦点领域：COBIT 核心模型

描述

及时有效地响应用户请求并处理所有类型的事故。恢复正常服务；记录并满足用户请求；记录、调查、诊断、上报和处理事故。

目的

通过快速解决用户查询和事件来实现生产力的提升和最大程度减少中断。评估变更影响并处理服务事故。处理用户请求并在事故后恢复服务。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标		一致性目标
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化	→	AG05 提供符合业务需求的 I&T 服务
企业目标的指标示例		**一致性目标的指标示例**
EG01 a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间		AG05 a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG08 a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		

A. 组件：流程

管理实践	指标示例
DSS02.01 定义事故和服务请求的分类方案。 定义事故和服务请求的分类方案和模式。	a. 每个优先级的服务请求和事故的总数量 b. 已上报事故的总数量

活动	能力级别
1. 定义事故和服务请求的分类和优先级方案，以及问题登记标准。使用此信息来确保以一致的方式处理和通知用户相关问题并进行趋势分析。	3
2. 定义已知错误的事故模式，以实现有效且高效的解决过程。	
3. 根据服务请求类型定义服务请求模式，以针对标准请求实现高效的自助式服务。	
4. 定义事故上报规则和流程，尤其针对重大事故和安全事故。	
5. 定义事故和请求的知识源，并描述它们的使用方法。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	IA.IP Implement Incident Investigation Processes
HITRUST CSF，第 9 版，2017 年 9 月	11.01 Reporting Information Security Incidents and Weaknesses
ISF, The Standard of Good Practice for Information Security 2016	TM2 Security Incident Management
ISO/IEC 20000-1:2011(E)	8.1 Incident and service request management
ISO/IEC 27002:2013/Cor.2:2015(E)	16. Information security incident management

A. 组件：流程（续）	
管理实践	**指标示例**
DSS02.02 对请求和事故进行记录、分类并确定优先级。 对服务请求和事故进行识别、记录和分类，并根据业务关键性和服务协议分配优先级。	a. 为记录服务请求和事故而定义的类型和类别的数量 b. 未分类的服务请求和事故的数量

活动	能力级别
1. 将所有服务请求和事故记录在日志中，包括所有相关信息，以便有效处理并维护完整的历史记录。	2
2. 为进行趋势分析，应确定类型和类别，对服务请求和事故进行分类。	
3. 根据 SLA 中对业务影响和紧迫性的服务定义，确定服务请求和事故的优先级。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
DSS02.03 验证、批准并履行服务请求。 选择适当的请求程序并验证服务请求是否满足定义的请求标准。获得必要的批准并履行服务请求。	a. 处理每种类型的服务请求的平均耗时 b. 满足定义的请求标准的服务请求的百分比

活动	能力级别
1. 在可能的情况下，使用预定义的流程步骤和标准变更来验证对服务请求申请的权限。	2
2. 针对议定的标准变更，获得财务和职能部门的批准或签字（如需要），或预定义批准。	
3. 执行选定的请求程序来满足服务请求。在可能的情况下，使用自助式自动菜单和预定义的请求模式来处理频繁请求的事项。	3

相关指南（标准、框架、合规性要求）	详细参考
ITIL 第 3 版，2011 年	Service Operation, 4.3 Request Fulfilment

管理实践	指标示例
DSS02.04 调查、诊断并分配事故。 识别并记录事故征兆，确定可能的原因，并分配给相关人员加以解决。	a. 已识别和记录的事故征兆的数量 b. 正确地确定征兆的原因数量 c. 参考日志中的重复问题的数量

活动	能力级别
1. 识别并描述相关征兆，以确定最可能的事故原因。参考可用的知识资源（包括已知的错误和问题）来识别可能的事故解决方案（临时方案和/或永久解决方案）。	2
2. 如果相关问题或已知错误尚不存在，并且事故满足议定的问题登记标准，应将新问题记录在日志中。	
3. 如需更深入的专业知识，应将事故分配给专家职能代表。必要时请联络适当层级的管理人员。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
DSS02.05 解决问题并从事故中恢复。 记录、应用和测试识别的解决方案或临时方案。采取恢复行动来恢复 I&T 相关服务。	a. 在议定的 SLA 内解决的事故的百分比 b. 利益相关方对事故解决和恢复感到满意的百分比

活动	能力级别
1. 选择并应用最合适的事故解决方案（临时方案和/或永久解决方案）。	2
2. 记录是否采用了变通方案来处理事故。	
3. 必要时采取恢复行动。	
4. 记录事故解决方案，并评估该解决方案是否可用作未来的知识源。	

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
ITIL 第 3 版，2011 年	Service Operation, 4.2 Incident Management
美国国家标准与技术研究所，Framework for Improving Critical Infrastructure Cybersecurity，第 1.1 版，2018 年 4 月	RC.RP Recovery Planning
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.9 Incident response (IR-4, IR-5, IR-6)
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，201 年 8 月	CSC 19： Incident Response and Management
管理实践	**指标示例**
DSS02.06 关闭服务请求和事故。 验证是否已满意地解决事故和/或满足服务请求，并关闭服务请求和事故。	a. 用户对服务请求履行的满意度水平 b. 在议定/可接受的时限内解决的事故的百分比

活动	能力级别
1. 与受影响的用户确认服务请求是否已圆满完成，或事故是否在议定/可接受的时限内得到满意的解决。	2
2. 关闭服务请求和事故。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	
管理实践	**指标示例**
DSS02.07 跟踪状态并生成报告。 定期跟踪、分析和报告事故状态以及请求履行的情况。分析趋势，为持续改进提供信息。	a. I&T 促成的服务的平均事故间隔时间 b. 造成关键业务流程中断的事故的数量和百分比

活动	能力级别
1. 监控和跟踪事故上报和解决方案以及请求处理程序，以推进事故或请求的解决或完成。	2
2. 识别信息的利益相关方及其对数据或报告的需求。确定报告频率和媒介。	3
3. 及时生成和分发报告或提供受控的在线数据访问。	4
4. 按类别和类型分析事故和服务请求。建立趋势并识别反复出现的问题的模式、SLA 违规或效率低下问题。	
5. 将该信息作为持续改进计划的输入。	5

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	MI.IM Ensure Incident Mitigation; IR.IR Incident Reporting
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.9 Incident response (IR-7, IR-8)

B. 组件：组织结构							
关键管理实践	首席技术官	业务流程所有者	开发总监	IT 运营总监	服务经理	信息安全经理
DSS02.01 定义事故和服务请求的分类方案。	A		R	R	R	
DSS02.02 对请求和事故进行记录、分类并确定优先级。	A			R	R	
DSS02.03 验证、批准并履行服务请求。	A	R	R	R	R	
DSS02.04 调查、诊断并分配事故。	A	R		R	R	
DSS02.05 解决问题并从事故中恢复。	A		R	R	R	R
DSS02.06 关闭服务请求和事故。	A			R	R	R
DSS02.07 跟踪状态并生成报告。	A			R	R	

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 27002:2013/Cor.2:2015(E)	16.1.1 Responsibilities and procedures

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
DSS02.01 定义事故和服务请求的分类方案。	APO09.03	SLA	问题登记标准	DSS03.01
	BAI10.02	配置贮存库	事故上报规则	内部
	BAI10.03	更新的配置项贮存库	事故和服务请求的分类方案和模式	内部
	BAI10.04	配置状态报告		
	DSS01.03	资产监控规则和事件条件		
	DSS03.01	问题分类方案		
	DSS04.03	事故响应行动和沟通		
DSS02.02 对请求和事故进行记录、分类并确定优先级。	APO09.03	SLA	已分类并排定优先级的事故和服务请求	APO08.03；APO09.04；APO13.03；DSS03.05
	BAI04.05	紧急情况上报程序	事故和服务请求日志	内部；MEA04.07
	DSS01.03	• 资产监控规则和事件条件 • 事故单		
	DSS05.07	安全相关的事故单		

C. 组件：信息流和信息项（另请参阅第 3.6 节）（续）				
管理实践	输入		输出	
DSS02.03 验证、批准并履行服务请求。	自	描述	描述	至
	APO12.06	风险相关的根本原因	已批准的服务请求	BAI06.01
			履行的服务请求	内部
DSS02.04 调查、诊断并分配事故。	BAI07.07	补充性支持计划	问题日志	DSS03.01
			事故征兆	内部
DSS02.05 解决问题并从事故中恢复。	APO12.06	风险相关事故的响应计划	事故解决方案	DSS03.03；DSS03.04；DSS03.05；MEA04.07
	DSS03.03	已知错误记录		
	DSS03.04	所学知识的沟通		
DSS02.06 关闭服务请求和事故。	DSS03.04	已关闭的问题记录	用户确认对服务的履行或问题的解决感到满意	APO08.03
			已关闭的服务请求和事故	APO08.03；APO09.04；DSS03.04
DSS02.07 跟踪状态并生成报告。	APO09.03	OLA	事故状态和趋势报告	APO08.03；APO09.04；APO11.04；APO12.01；MEA01.03
	DSS03.01	问题状态报告	请求履行状态和趋势报告	APO08.03；APO09.04；APO11.04；MEA01.03
	DSS03.02	问题解决报告		
	DSS03.05	问题解决监控报告		
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
应用程序支持	Skills Framework for the Information Age，第 6 版，2015 年	ASUP
客户服务支持	Skills Framework for the Information Age，第 6 版，2015 年	CSMG
事故管理	Skills Framework for the Information Age，第 6 版，2015 年	USUP
网络支持	Skills Framework for the Information Age，第 6 版，2015 年	NTAS
用户支持	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	C. Run—C.1. User Support

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
服务请求政策	陈述理由并为服务和事故请求及其文档记录提供指南。	ITIL 第 3 版，2011 年	Service Operation, 3. Service operation principles

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
使员工能够正确、及时地识别事故并选择适当的上报途径。鼓励预防。立即响应并解决事故。避免英雄主义文化。		

G. 组件：服务、基础设施和应用程序
事故跟踪工具和系统

领域：交付、服务与支持 管理目标：DSS03 — 妥当管理的问题	焦点领域：COBIT 核心模型

描述

识别问题及其根本原因并进行分类。及时提供解决方案，以防事故再次发生。提供改进建议。

目的

通过减少运营问题来提高可用性和服务水平，降低成本，提高客户的便利度和满意度，以及通过确定根本原因协助解决问题。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标		一致性目标	
• EG01 有竞争力的产品和服务的组合 • EG08 内部业务流程功能的优化	→	AG05	提供符合业务需求的 I&T 服务
企业目标的指标示例		**一致性目标的指标示例**	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG05	a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		

A. 组件：流程

管理实践	指标示例
DSS03.01 识别问题并进行分类。 定义并实施标准和程序来识别和报告问题，包括对问题分类和确定优先级。	a. 已记录问题的重大事故的百分比 b. 已根据议定的 SLA 解决的事故的百分比 c. 已适当识别（包括分类和确定优先级）的问题的百分比

活动	能力级别
1. 通过事故报告、错误日志和其他问题识别资源之间的关联来识别问题。	2
2. 正式处理所有问题并访问所有相关数据。这些数据包括来自 IT 变更管理系统的信息以及 IT 配置/资产和事故详细信息。	
3. 定义适当的支持团队来协助识别问题、分析根本原因以及确定解决方案，为问题管理提供支持。根据预定义的类别（例如硬件、网络、软件、应用程序和支持软件）确定支持团队。	
4. 通过与业务部门磋商来定义优先级，以确保根据议定的 SLA 及时识别问题并分析根本原因。基于业务影响和紧迫性确定优先级。	
5. 向服务台报告已识别问题的状态，以及时向客户和 IT 管理层传达相关情况。	
6. 维护一个问题管理目录，以登记和报告已识别的问题。使用该目录建立问题管理流程的审计轨迹，包括每个问题的状态（即“开单”、“重开单”、“进行中”或“关单”）。	

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 20000-1:2011(E)	8.2 Problem management

A. 组件：流程（续）	
管理实践	**指标示例**
DSS03.02 调查和诊断问题。 使用相关的主题专家来调查和诊断问题，以评估和分析根本原因。	a. 分类为“已知错误”的已识别的问题的数量 b. 在整个生命周期中得到调查和诊断的问题的数量

活动	能力级别
1. 将事故数据与已知和可疑错误的数据库（例如外部供应商传达的数据）进行比较，确定问题是否属于已知错误。将问题归类为“已知错误”。	3
2. 将受影响的配置项与已建立/已知错误相关联。	
3. 产生报告以沟通问题解决的进展并监控未解决问题的持续影响。在整个生命周期内监控问题处理流程的状态，包括来自 IT 变更和配置管理的输入。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
DSS03.03 记录已知错误。 确定了问题的根本原因后，尽快创建已知错误记录，记录适当的临时方案，并确定可能的解决方案。	a. 已通过满意的解决方案来处理根本原因的问题的数量 b. 利益相关方对识别根本原因、创建已知错误记录和适当的临时方案以及确定可能的解决方案感到满意的百分比

活动	能力级别
1. 确定了问题的根本原因后，尽快创建已知错误记录并制定合适的临时方案。	2
2. 根据成本/效益业务案例以及业务影响和紧迫性，确定和评估已知错误的解决方案，并确定优先级和加以处理（通过 IT 变更管理）。	3

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
DSS03.04 解决并关闭问题。 识别并启动能够解决根本原因的可持续解决方案。必要时通过既定的变更管理流程提出变更请求来解决错误。确保受影响的人员了解采取的行动和制定的计划，防止未来发生事故。	a. 因未解决的问题导致的反复发生的事故的减少数量 b. 为待解决的问题定义临时方案的百分比

活动	能力级别
1. 在确认成功消除已知错误之后，或在与业务部门就如何通过其他方式处理问题达成协议之后关闭问题记录。	2
2. 通知服务台问题关闭的时间表（例如，修复已知错误的时间表、可能的临时方案，或问题将存续至实施变更之后的事实）以及所采取方法的后果。适当地向受影响的用户和客户传达相关情况。	
3. 在整个解决流程中，获取 IT 变更管理团队提供的有关问题和错误解决进度的定期报告。	3
4. 监控问题和已知错误对服务的持续影响。	4
5. 审查并确认重大问题是否得到成功解决。	
6. 确保将审查期间学到的知识融汇到与业务客户进行的服务审查会议。	5

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
DSS03.05 执行主动问题管理。 收集并分析运营数据（特别是事故和变更记录）来确定可能意味着问题的新兴趋势。将问题记录在日志中以便进行评估。	a. 在主动问题管理活动中记录的问题的百分比 b. 关键利益相关方对 IT 变更和事故相关问题的信息沟通感到满意的百分比

活动	能力级别
1. 捕获 I&T 变更和事故相关的问题信息，并传达给关键利益相关方。通过报告和定期会议与事故、问题、变更和配置管理流程所有者进行沟通，考虑近期问题和潜在的纠正措施。	3
2. 确保事故、问题、变更和配置管理流程的所有者和管理人员定期召开会议，讨论已知问题和计划的未来变更。	
3. 识别并启动能够解决根本原因的可持续解决方案（永久修复）。通过既定的变更管理流程提出变更请求。	
4. 为了使企业能够监控问题的总成本，应捕获问题管理流程活动（例如修复问题和已知错误）所产生的变更工作并进行报告。	4
5. 生成报告，根据业务要求和 SLA 监控问题解决方案。确保正确地上报问题，例如根据议定的标准上报给更高管理层、联系外部供应商，或告知变更咨询委员会，以提高旨在实施临时变通方案的紧急变更申请 (RFC) 的优先级。	
6. 为优化资源利用并减少临时方案，应跟踪问题趋势。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	MI.IC Ensure Incident Containment
ITIL 第 3 版，2011 年	Service Operation, 4.4 Problem Management

B. 组件：组织结构							
关键管理实践	**执行委员会**	**首席信息官**	**首席技术官**	**开发总监**	**IT 运营总监**	**服务经理**	**信息安全经理**
DSS03.01 识别问题并进行分类。		R	A	R	R	R	
DSS03.02 调查和诊断问题。			A		R	R	R
DSS03.03 记录已知错误。			A		R	R	R
DSS03.04 解决并关闭问题。			A		R	R	
DSS03.05 执行主动问题管理。	R		A		R	R	

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
DSS03.01 识别问题并进行分类。	自	描述	描述	至
	APO12.06	风险相关的根本原因	问题分类方案	DSS02.01
	DSS02.01	问题登记标准	问题状态报告	DSS02.07
	DSS02.04	问题日志	问题登记表	内部
DSS03.02 调查和诊断问题。	APO12.06	风险相关的根本原因	问题解决报告	DSS02.07
			问题的根本原因	内部；DSS03.05
DSS03.03 记录已知错误。	APO12.06	风险相关的根本原因	针对已知错误建议的解决方案	BAI06.01
	DSS02.05	事故解决方案	已知错误记录	DSS02.05
DSS03.04 解决并关闭问题。	DSS02.05	事故解决方案	所学知识的沟通	APO08.04；DSS02.05
	DSS02.06	已关闭的服务请求和事故	已关闭的问题记录	DSS02.06
DSS03.05 执行主动问题管理。	APO12.06	风险相关的根本原因	确定的可持续的解决方案	BAI06.01
	DSS02.02	• 对事故和服务请求进行了分类并确定了优先级 • 事故解决方案	问题解决监控报告	DSS02.07；MEA04.07
	DSS03.04	问题的根本原因		
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
应用程序支持	Skills Framework for the Information Age，第 6 版，2015 年	ASUP
网络支持	Skills Framework for the Information Age，第 6 版，2015 年	NTAS
问题管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	C. Run—C.4. Problem Management
问题管理	Skills Framework for the Information Age，第 6 版，2015 年	PBMG

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
问题解决政策	记录理由并提供指南，以解决事故导致的问题和确定经验证的变通方案。	ITIL 第 3 版，2011 年	Service Operation, 3. Service operation principles

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
支持具有明确定义的角色和职责的主动问题管理（检测、行动和预防）文化。通过提供独立的报告机制和/或奖励提出问题的人员，确保营造透明和开放的环境来鼓励报告问题。		

G. 组件：服务、基础设施和应用程序
问题跟踪/解决系统

领域：交付、服务与支持 管理目标：DSS04 — 妥当管理的连续性	焦点领域：COBIT 核心模型

描述

制定并维护一份行之有效的计划，使业务部门和 IT 机构能够对事故做出响应并在发生业务中断时做出快速调整，这样能保证关键业务流程和所需 I&T 服务的继续运行，并能将资源、资产和信息的可用性保持在企业可接受的水平之上。

目的

在发生重大中断事件（例如威胁、机会、要求）时，快速调整，维持业务运营，并将资源和信息的可用性保持在企业可接受的水平之上。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG02 妥当管理的业务风险 • EG06 业务服务连续性和可用性 • EG08 内部业务流程功能的优化	• AG05 提供符合业务需求的 I&T 服务 • AG07 信息、参与执行的基础设施和应用程序的安全，以及隐私的安全

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG05	a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG02	a. 风险评估涵盖的关键业务目标和服务的百分比 b. 风险评估未发现的重大事故数量与总事故数量的比率 c. 风险概况的更新频率	AG07	a. 导致财务损失、业务中断或公众形象受损的保密性事故的数量 b. 导致财务损失、业务中断或公众形象受损的可用性事故的数量 c. 导致财务损失、业务中断或公众形象受损的完整性事故的数量
EG06	a. 导致重大事故的客户服务或业务流程中断的次数 b. 事故的业务成本 c. 因计划外服务中断而损失的业务处理小时数 d. 与承诺的服务可用性目标有关的投诉百分比		
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		

A. 组件：流程	
管理实践	**指标示例**
DSS04.01 定义业务连续性政策、目标和范围。 定义与企业和利益相关方目标相一致的业务连续性政策和范围，以提高业务弹性。	a. 因不当辨识的流程和活动而重定的业务连续性目标和范围的百分比 b. 参与、定义和商定连续性政策和范围的关键利益相关方的百分比

活动	能力级别
1. 确定对企业运营至关重要的、或必须符合法律规定、合同义务的内部和外包业务流程及服务活动。	2
2. 确定定义和商定连续性政策和范围的关键利益相关方及其角色和职责。	
3. 定义并记录商定的业务弹性最低政策目标和范围。	
4. 确定必要的支持业务流程和相关 I&T 服务。	

相关指南（标准、框架、合规性要求）	详细参考
HITRUST CSF，第 9 版，2017 年 9 月	12.01 Information Security Aspects of Business Continuity Management
ISF, The Standard of Good Practice for Information Security 2016	BC1.1 Business Continuity Strategy; BC1.2 Business Continuity Programme
ISO/IEC 27002:2013/Cor.2:2015(E)	17. Information security aspects of business continuity management
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.6 Contingency planning (CP-1)

管理实践	指标示例
DSS04.02 维护业务恢复能力。 评估业务恢复能力选项，并选择具有成本效益且可行的战略，以确保在面对灾难或其他重大事故或中断时企业的连续性、灾难恢复和事故响应能力。	a. 重大事故或中断导致的总停机时间 b. 参与业务影响分析（评估中断对关键业务功能的长期影响以及中断将对他们产生的影响）的关键利益相关方的百分比

活动	能力级别
1. 确定可能导致重大破坏性事故的潜在场景。	2
2. 开展业务影响分析以评估中断对关键业务功能的长期影响以及中断将对关键利益相关方产生的影响。	
3. 基于可接受的业务中断时长和可承受的最长中断时间来设定恢复业务流程和支持性 I&T 所需的最短时间。	
4. 确定将导致启动连续性计划的条件和关键决策所有者。	
5. 评估出现可能导致丧失业务连续性的威胁的可能性。确定相应措施，通过提高预防和恢复能力来降低发生此类威胁的可能性及其产生的影响。	3
6. 分析连续性要求以确定可能的战略性业务和技术方案。	
7. 确定各个战略性技术方案的资源需求和成本并提出战略性建议。	
8. 获得执行管理层对所选战略方案的批准。	

相关指南（标准、框架、合规性要求）	详细参考
ISF, The Standard of Good Practice for Information Security 2016	BC1.3 Resilient Technical Environments
ITIL 第 3 版，2011 年	Service Design, 4.6 IT Continuity Management
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.6 Contingency planning (CP-2)

A. 组件：流程（续）	
管理实践	**指标示例**
DSS04.03 制定并实施业务连续性应对措施。 根据战略制定业务连续性计划 (BCP) 和灾难恢复计划 (DRP)。记录所有必需的程序，使企业在发生事故时能够继续开展关键活动。	a. 未被计划涵盖的关键业务系统的数量 b. 参与制定 BCP 和 DRP 的关键利益相关方的百分比

活动	能力级别
1. 定义在发生中断时应采取的事故响应行动和沟通。定义相关的角色和职责，包括政策和实施的责任。	2
2. 确保关键供应商和外包合作伙伴实施了有效的连续性计划。根据需要获取审计证据。	
3. 定义实现业务流程恢复的条件和恢复程序。包括信息数据库的更新和对账，以维护信息完整性。	
4. 制定并维护可运作的 BCP 和 DRP，其中包含为实现关键业务流程的持续运营和/或临时流程安排而应遵循的程序，包括外包服务提供商计划的链接。	
5. 定义并记录支持连续性和恢复程序所需的资源，包括人员、设施和 IT 基础设施。	
6. 定义并记录支持计划所需的信息备份要求，包括计划、纸质文档以及数据文件。考虑安全和异地存储需求。	
7. 确定参与执行计划和程序的人员应具备的技能。	
8. 将计划和支持文档安全地分发给获得相应授权的相关方。确保在所有灾难场景中都可以访问计划和文档。	3

相关指南（标准、框架、合规性要求）	详细参考
ISF, The Standard of Good Practice for Information Security 2016	BC1.4 Crisis Management; BC2.1 Business Continuity Planning
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.6 Contingency planning (CP-6, CP-9, CP-10)

管理实践	指标示例
DSS04.04 演练、测试和审查业务连续性计划 (BCP) 和灾难响应计划 (DRP)。 定期测试连续性，以根据预定结果进行计划演练、维护业务恢复能力，以及推动创新解决方案的开发。	a. 测试的频率 b. 已实现恢复目标的演练和测试的数量

活动	能力级别
1. 定义计划在业务、技术、物流、管理、程序和运营系统方面的演练和测试目标，以验证 BCP 和 DRP 在管理业务风险方面的完整性。	2
2. 定义和商定切实可行的利益相关方演练并验证连续性程序，包括角色和职责以及使业务流程中断最小化的数据保留安排。	
3. 分配执行连续性计划演练和测试的角色和职责。	
4. 根据连续性计划安排演练和测试活动。	3
5. 开展演练后汇报和分析以衡量成果。	4
6. 根据审查结果提出改进当前连续性计划的建议。	5

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	PP.RS Develop and Maintain Response Plans; PP.RP Develop and Maintain Recovery Plans
ISF, The Standard of Good Practice for Information Security 2016	BC2.3 Business Continuity Testing
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 20: Penetration Tests and Red Team Exercises

A. 组件：流程（续）	
管理实践	**指标示例**
DSS04.05 审查、维护和改进连续性计划。 定期进行连续性能力的管理审查，以确保其持续适用性、充分性和有效性。根据变更控制流程管理计划变更，确保连续性计划保持最新并持续反映实际业务要求。	a. 在计划中已经体现的议定计划改进的百分比 b. 保持更新的业务连续性计划和业务影响评估的百分比

活动	能力级别
1. 根据所作的所有假设以及当前的业务运营和战略目标，定期业务审查连续性计划和业务连续性能力。	3
2. 定期审查连续性计划，以考虑新的或重大变更对企业组织、业务流程、外包安排、技术、基础设施、操作系统和应用系统的影响。	
3. 考虑是否需要修订业务影响评估（具体取决于变更的性质）。	
4. 提出政策、计划、程序、基础设施以及角色和职责方面的变更建议。通过 IT 变更管理流程适当地沟通这些建议，以获得管理层的批准并执行。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
DSS04.06 开展连续性计划培训。 面向所有内外部相关方，提供关于中断情况下的程序以及他们的角色和职责的定期培训课程。	a. 已接受培训的内外部利益相关方的百分比 b. 具备最新技能和能力的内外部相关方的百分比

活动	能力级别
1. 推广 BCP 和 DRP 意识及培训。	2
2. 定义和维护面向执行连续性计划、影响评估、风险评估、媒体沟通和事故响应的人员的培训要求和计划。确保培训计划充分考虑培训的频率和授课机制。	3
3. 根据实践培训来培养相关能力，包括参加演练和测试。	
4. 基于演练和测试结果监控技能和能力。	4

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.6 Contingency planning (CP-4)

管理实践	指标示例
DSS04.07 管理备份安排。 保持业务关键信息的可用性。	a. 安全送达并保管的备份介质的百分比 b. 从备份或备用介质副本成功并及时恢复的百分比

活动	能力级别
1. 根据事先制定的日程表备份系统、应用程序、数据和文档。考虑备份频率（每月、每周、每天等）、备份模式（例如用于实时备份的磁盘镜像和用于长期保留的 DVD-ROM）、备份类型（例如完整备份与增量备份）以及备份介质类型。另外还应考虑自动在线备份、数据类型（例如语音、光学）、创建日志、最终用户的重要计算数据（例如电子表格）、数据源的物理和逻辑位置、安全性和访问权限，以及加密。	2
2. 定义符合业务需求的现场和异地存储的备份数据要求。考虑备份数据所需的可访问性。	
3. 定期测试和更新存档和备份的数据。	
4. 确保由第三方维护或处理的系统、应用程序、数据和文档已得到适当备份或其他方式的保护。考虑要求第三方返还备份。考虑托管或存放安排。	

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI Cybermaturity Platform，2018 年	IP.BP Apply Backup Processes
HITRUST CSF，第 9 版，2017 年 9 月	09.05 Information Back-Up
ISF, The Standard of Good Practice for Information Security 2016	SY2.3 Backup
ISO/IEC 27002:2013/Cor.2:2015(E)	12.3 Backup
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.6 Contingency planning (CP-3)
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 10: Data Recovery Capability
管理实践	**指标示例**
DSS04.08 开展恢复后审查。 在成功恢复被中断的业务流程和服务之后，评估业务连续性计划 (BCP) 和灾难响应计划 (DRP) 的充分性。	a. 在计划中确定并随后解决的问题的百分比 b. 在培训材料中确定并随后解决的问题的百分比

活动	能力级别
1. 评估对已成文的 BCP 和 DRP 的遵循情况。	4
2. 确定计划的有效性、连续性能力、角色和职责、技能和能力、事故后恢复能力、技术基础设施以及组织结构和相互关联。	
3. 识别计划和能力的弱点或疏漏并提出改进建议。获得管理层对计划变更的批准，并通过企业变更控制流程执行变更。	5

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构														
关键管理实践	**执行委员会**	**首席运营官**	**首席信息官**	**首席技术官**	**首席信息安全官**	**业务流程所有者**	**数据管理职能部门**	**架构总监**	**开发总监**	**IT 运营总监**	**服务经理**	**信息安全经理**	**业务连续性经理**
DSS04.01 定义业务连续性政策、目标和范围。	R	A	R		R	R				R	R		R
DSS04.02 维护业务恢复能力。	R	A	R			R		R		R		R	R
DSS04.03 制定并实施业务连续性应对措施。			R	R		R				R		R	A
DSS04.04 演练、测试和审查业务连续性计划 (BCP) 和灾难响应计划 (DRP)。			R	R		R				R		R	A
DSS04.05 审查、维护和改进连续性计划。		A	R	R	R	R				R			R
DSS04.06 开展连续性计划培训。			R	R		R			R	R		R	A
DSS04.07 管理备份安排。				A			R			R		R	R
DSS04.08 开展恢复后审查。			R	R	R	R				R			A

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
DSS04.01 定义业务连续性政策、目标和范围。	APO09.03	SLA	业务连续性政策和目标	APO01.02
			评估当前连续性能力和差距	内部
			破坏性事故场景	内部
DSS04.02 维护业务恢复能力。	APO12.06	• 风险影响的沟通 • 风险相关的根本原因	获得批准的战略方案	APO02.05
			BIA	APO12.02
			连续性要求	内部
DSS04.03 制定并实施业务连续性应对措施。	APO09.03	OLA	事故响应行动和沟通	DSS02.01
			BCP	内部
DSS04.04 演练、测试和审查业务连续性计划 (BCP) 和灾难响应计划 (DRP)。			测试结果和建议	内部
			测试演练	内部
			测试目标	内部
DSS04.05 审查、维护和改进连续性计划。			建议的计划变更	内部
			计划的审查结果	内部
DSS04.06 开展连续性计划培训。	人力资源	要求培训的人员名单	技能和能力的监控结果	APO07.03
			培训要求	APO07.03
DSS04.07 管理备份安排。	APO14.10	• 备份计划 • 备份测试计划	备份数据的测试结果	内部
			备份数据	内部；APO14.08
DSS04.08 开展恢复后审查。			已批准的计划变更	BAI06.01
			恢复后审查报告	内部

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
连续性管理	Skills Framework for the Information Age，第 6 版，2015 年	COPL

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
业务连续性政策	概述管理层在以下方面的承诺：业务影响评估 (BIA)、业务应急计划（包括可信恢复）、关键系统的恢复要求、突发情况的规定阈值和触发条件、升级上报计划、数据恢复计划，以及培训和测试。		
危机管理政策	设定关键风险领域的危机响应准则和顺序。除了 I&T 安全、网络管理以及数据安全和隐私，危机管理也是完整的 I&T 风险管理应考虑的运营级策略之一。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
将对业务恢复能力的需求融入到企业文化中。定期、频繁地向员工传达最新的核心价值观、理想的规范行为和战略目标，使企业在任何情况下都能保持沉着镇定的形象。定期测试业务连续性程序和灾难恢复计划。		

G. 组件：服务、基础设施和应用程序
• 外部托管服务 • 事故监控工具 • 远程储存设施服务

领域：交付、服务与支持 管理目标：DSS05 — 妥当管理的安全服务	焦点领域：COBIT 核心模型

描述

根据安全政策保护企业信息，将信息安全风险保持在企业可接受的水平。建立和维护信息安全角色及访问特权。执行安全监控。

目的

最大程度降低运营信息安全漏洞和事故对业务活动造成的影响。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG02 妥当管理的业务风险 • EG06 业务服务连续性和可用性	• AG02 妥当管理的 I&T 相关风险 • AG07 信息、参与执行的基础设施和应用程序的安全，以及隐私的安全
企业目标的指标示例	**一致性目标的指标示例**
EG02 a. 风险评估涵盖的关键业务目标和服务的百分比 b. 风险评估未发现的重大事故数量与总事故数量的比率 c. 风险概况的更新频率	AG02 a. 风险概况的更新频率 b. 涵盖 I&T 相关风险的企业风险评估的百分比 c. 风险评估中未识别的 I&T 相关重大事故的数量
EG06 a. 导致重大事故的客户服务或业务流程中断的次数 b. 事故的业务成本 c. 因计划外服务中断而损失的业务处理小时数 d. 与承诺的服务可用性目标有关的投诉百分比	AG07 a. 导致财务损失、业务中断或公众形象受损的保密性事故的数量 b. 导致财务损失、业务中断或公众形象受损的可用性事故的数量 c. 导致财务损失、业务中断或公众形象受损的完整性事故的数量

A. 组件：流程

管理实践	指标示例
DSS05.01 防范恶意软件侵害。 在整个企业中实施和维护预防、检测和更正措施（特别是最新的安全补丁和病毒控制措施）来保护信息系统和技术免受恶意软件（例如勒索软件、恶意代码、病毒、蠕虫、间谍软件、垃圾邮件）侵害。	a. 被恶意软件攻击成功的次数 b. 未通过恶意软件攻击测试（例如网络钓鱼电子邮件测试）的员工的百分比

活动	能力级别
1. 在所有处理设施上安装并激活恶意软件防范工具，根据需要更新恶意软件定义文件（自动或半自动）。	2
2. 过滤入站流量，例如电子邮件和下载，以防范未经请求的信息（例如间谍软件、网络钓鱼电子邮件）。	
3. 传播防范恶意软件的意识并强制实施防范程序和防范职责。定期举办关于如何处理在使用电子邮件和互联网过程中遇到恶意软件的培训。培养用户养成不要随意打开可疑邮件的习惯，而应该向有关部门报告，也不要安装共享或未经批准的软件。	3
4. 使用集中配置和 IT 变更管理集中分发所有防护软件（版本和补丁级别）。	
5. 定期审查和评估关于新的潜在威胁的信息（例如审查供应商产品和服务的安全公告）。	4

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	DP.DC Detect Malicious Code; RI.VT Vulnerability and Threat Identification
HITRUST CSF，第 9 版，2017 年 9 月	09.04 Protection Against Malicious & Mobile Code
SF, The Standard of Good Practice for Information Security 2016	TS1 Security Solutions
SO/IEC 27002:2013/Cor.2:2015(E)	12.2 Protection against malware
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 4: Continuous Vulnerability Assessment and Remediation; CSC 8: Malware Defenses

A. 组件：流程（续）	
管理实践	**指标示例**
DSS05.02 管理网络和连接安全性。 使用安全措施和相关的管理程序来保护所有连接方式得到的信息。	a. 防火墙遭到破坏的次数 b. 已发现的漏洞数量 c. 由于安全事故造成网络和系统无法使用的时间百分比

活动	能力级别
1. 仅允许获得授权的设备访问公司信息和企业网络。这些设备应被设置成需要强制输入密码。	2
2. 实施网络过滤机制，如防火墙和入侵检测软件。实施适当的策略来控制入站和出站流量。	
3. 将获得批准的安全协议应用于网络连接。	
4. 以安全的方式配置网络设备。	
5. 根据信息分类对其在传输时进行加密。	3
6. 根据风险评估和业务要求建立并维护安全连接的策略。	
7. 建立可信机制来支持信息的安全传输和接收。	
8. 定期开展渗透测试以确定网络保护的充分性。	4
9. 定期开展系统安全测试以确定系统保护的充分性。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	AC.MI Manage Network Integrity & Segregation; CM.MN Monitor Networks; AC.CP Manage Communication Protections
HITRUST CSF，第 9 版，2017 年 9 月	01.04 Network Access Control
ISF, The Standard of Good Practice for Information Security 2016	PA2.3 Mobile Device Connectivity; NC1.1 Network Device Configuration
ISO/IEC 27002:2013/Cor.2:2015(E)	13.1 Network security management
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.20 System and information integrity (SI-8)
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 9: Limitation and Control of Network Ports, Protocols, and Services; CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

管理实践	指标示例
DSS05.03 管理终端安全性。 确保终端（例如，笔记本电脑、台式机、服务器以及其他移动和网络设备或软件）受保护的程度等于或高于为所处理、存储或传输的信息所定义的安全要求。	a. 涉及终端设备的事故的数量 b. 在网络上或在最终用户环境中检测到的未经授权设备的数量 c. 接受有关终端设备使用的意识培训的员工百分比

活动	能力级别
1. 以安全的方式配置操作系统。	2
2. 实施设备锁定机制。	
3. 管理远程访问和控制（例如移动设备、远程办公）。	
4. 以安全的方式管理网络配置。	
5. 在终端设备实施网络流量过滤。	
6. 保护系统的完整性。	
7. 为终端设备提供物理保护。	
8. 安全地处置终端设备。	
9. 通过电子邮件和 Web 浏览器管理恶意访问，例如，阻止某些　　和停用智能手机点击打开链接的功能。	
10. 根据信息分类对其存储进行加密。	3

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI Cybermaturity Platform，2018 年	IP.MM Apply Mobile Device Management; TP.MP Apply Media Protection; DP.DP Detect Mobile Code and Browser Protection
ISF, The Standard of Good Practice for Information Security 2016	PM1.3 Remote Working; PA2.1 Mobile Device Configuration; PA2.4 Employee-owned Devices; PA2.5 Portable Storage Devices; NC1.6 Remote Maintenance
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.4 Assessment, authorization and monitoring (CA-8, CA-9); 3.19 System and communications protection (SC-10)
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers; CSC 7: Email and Web Browser Protections
管理实践	**指标示例**
DSS05.04 管理用户身份和逻辑访问。 确保所有用户根据业务需求获取信息访问权限。与业务部门协调管理各自部门在业务流程中的访问权限。	a. 账户变更与更新之间的平均时间 b. 账户数量（对比获得授权的用户/员工数量） c. 与未经授权的信息访问相关的事故数量

活动	**能力级别**
1. 根据业务功能、流程要求和安全政策来维护用户访问权限。根据最小特权、按需拥有和按需知密的原则调整身份和访问权限的管理，使其符合定义的角色和职责。	2
2. 仅根据指定管理人员授权的已获批准和记录的交易来及时管理所有访问权限（创建、修改和删除）变更。	3
3. 分离特权用户账户、将其减少到所需的最小数量，并对其进行主动管理。确保对这些账户的所有活动进行监控。	
4. 按职能角色对所有信息处理活动进行唯一标识。与业务部门协调，确保按照一致的方式定义所有角色，包括由业务部门本身在业务流程应用程序内定义的角色。	
5. 根据个人角色或业务规则对所有信息资产的访问执行身份认证。与负责管理业务流程中所用应用程序内的身份认证的业务部门协调，确保身份认证控制得到适当的管理。	
6. 确保所有用户（内部、外部和临时用户）及其在 IT 系统（业务应用程序、IT 基础设施、系统操作、开发和维护）上的活动是可唯一识别的。	
7. 根据信息的敏感度和监管要求维护信息访问的审计轨迹。	4
8. 对所有账户和相关特权进行定期管理审查。	

相关指南（标准、框架、合规性要求）	**详细参考**
HITRUST CSF，第 9 版，2017 年 9 月	10.03 Cryptographic Controls
ISF, The Standard of Good Practice for Information Security 2016	PM1.1 Employment Life Cycle; SA1 Access Management
ISO/IEC 27002:2013/Cor.2:2015(E)	7.3 Termination and change of employment; 9. Access control
ITIL 第 3 版，2011 年	Service Operation, 4.5 Access Management
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.1 Access control (AC-11, AC-12); 3.11 Media protection (MP-2, MP-4, MP-7); 3.13 Physical and environmental protection (PE-2, PE-3, PE-6)
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 1: Inventory of Authorized and Unauthorized Devices; CSC 2: Inventory of Authorized and Unauthorized Software; CSC 5: Controlled Use of Administrative Privileges; CSC 16: Account Monitoring and Control

A. 组件：流程（续）	
管理实践	**指标示例**
DSS05.05 管理对 I&T 资产的物理访问。 根据业务需求定义和执行必要的程序（包括应急程序）来授予、限制和撤销对工作场所、建筑物和区域的访问权。对工作场所、建筑物和区域的访问应该有正当理由、经过授权、加以记录并受到监控。此要求适用于进入工作场所的所有人员，包括正式员工、临时员工、客户、供应商、访客或任何其他第三方人员。	a. 物理安全评估的平均评级 b. 物理信息安全相关事故的数量

活动	能力级别
1. 记录并监控 IT 站点的所有入口点。登记站点的所有访客，包括承包商和供应商。	2
2. 确保所有人员都必须在需要的时候出示已获得相应批准的出入证件。	
3. 访客在现场期间必须有人员全程陪同。	
4. 通过建立边界限制（例如栅栏、墙壁以及内门和外门上的安全设备）来限制和监控对敏感 IT 站点的访问。	
5. 访问授权的管理，对设备的访问必须获得相应的授权。	3
6. 确保访问配置文件保持最新。基于工作职能和职责的原则制定访问 IT 站点（服务器机房、建筑物或区域）的规则。	
7. 定期开展物理信息安全意识培训。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	AC.MA Manage Access; ID.DI Determine Impacts
HITRUST CSF，第 9 版，2017 年 9 月	01.01 Business Requirement for Access Control; 01.02 Authorized Access to Information Systems; 02.0 Human Resources Security
ISF, The Standard of Good Practice for Information Security 2016	NC1.2 Physical Network Management
ISO/IEC 27002:2013/Cor.2:2015(E)	11. Physical and environmental security

管理实践	指标示例
DSS05.06 管理敏感文档和输出设备。 对敏感 I&T 资产（例如特殊表单、可流通票据、特殊用途的打印机或安全令牌）采取适当的保护措施、会计惯例和库存管理。	a. 失窃的输出设备的数量 b. 已列入清单的敏感文档和输出设备的百分比

活动	能力级别
1. 建立规则，对敏感文件和输出设备在企业内外部的接收、使用、移除和处置进行治理。	2
2. 确保实施了加密控制，保护以电子方式存储的敏感信息。	
3. 根据最小特权原则分配敏感文档和输出设备的访问特权，从而平衡风险和业务要求。	3
4. 建立敏感文档和输出设备清单，并定期核对。	
5. 针对敏感文档建立适当的物理保护措施。	

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI Cybermaturity Platform，2018 年	CM.Ph Monitor Physical
HITRUST CSF，第 9 版，2017 年 9 月	01.06 Application & Information Access Control; 01.07 Mobile Computing & Teleworking; 08.0 Physical & Environmental Security; 10.03 Cryptographic Controls; 10.04 Security of System Files
ISF, The Standard of Good Practice for Information Security 2016	IR2.3 Business Impact Assessment - Confidentiality Requirements; IR2.4 Business Impact Assessment - Integrity Requirements; IR2.5 Business Impact Assessment - Availability Requirements; IM2.2 Sensitive Physical Information; PA2.2 Enterprise Mobility Man
ISO/IEC 27002:2013/Cor.2:2015(E)	10. Cryptography
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.1 Access control (AC-2, AC-3, AC-4, AC-5, AC-6, AC-13, AC-24); 3.7 Identification and authentication (IA-2, IA-10, IA-11)
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 15: Wireless Access Control
管理实践	**指标示例**
DSS05.07 管理漏洞并监控基础设施的安全相关事件。 使用工具和技术组合（例如入侵检测工具）来管理漏洞并监控基础设施中未经授权的访问。确保将安全工具、技术和检测整合到常规事件监控与事故管理中。	a. 对外围设备执行漏洞测试的次数 b. 测试期间发现的漏洞数量 c. 补救漏洞所花的时间 d. 监控系统在识别潜在的安全事故时及时创建事故单的百分比
活动	**能力级别**
1. 持续使用可支持的技术、服务和资产组合（例如漏洞扫描程序、模糊测试器和嗅探器、协议分析器）来识别信息安全漏洞。	2
2. 定义并了解风险场景，以便能够轻松识别风险场景并了解其可能性和影响。	
3. 定期审查事件日志中的潜在事故。	
4. 确保监控在识别潜在事故时及时创建安全相关的事故单。	
5. 记录安全相关的事件，并将记录适当保留一段时间。	3
相关指南（标准、框架、合规性要求）	**详细参考**
ISF, The Standard of Good Practice for Information Security 2016	IR2.6 Threat Profiling
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.7 Identification and authentication (IA-3); 3.11 Media protection (MP-1); 3.13 Physical and environmental protection (PE-5); 3.19 System and communications protection (SC-15)
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	Maintenance, Monitoring, and Analysis of Audit Logs

B. 组件：组织结构								
关键管理实践	首席信息官	首席信息安全官	业务流程所有者	人力资源总监	开发总监	IT 运营总监	信息安全经理	隐私官
DSS05.01 防范恶意软件侵害。		A	R	R	R	R	R	
DSS05.02 管理网络和连接安全性。		A			R	R	R	
DSS05.03 管理终端安全性。		A			R	R	R	
DSS05.04 管理用户身份和逻辑访问。		A	R			R	R	R
DSS05.05 管理对 I&T 资产的物理访问。		A				R	R	R
DSS05.06 管理敏感文档和输出设备。	A					R		R
DSS05.07 管理漏洞并监控基础设施的安全相关事件。		A				R	R	R

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
DSS05.01 防范恶意软件侵害。	自	描述	描述	至
			恶意软件预防政策	APO01.02
			潜在威胁的评估	APO12.02；APO12.03
DSS05.02 管理网络和连接安全性。	APO01.07	数据分类准则	连接安全政策	APO01.02
	APO09.03	SLA	渗透试验的结果	MEA04.07
DSS05.03 管理终端安全性。	APO03.02	信息架构模型	终端设备的安全政策	APO01.02
	APO09.03	• SLA • OLA		
	BAI09.01	实际库存检查的结果		
	DSS06.06	违规报告		
DSS05.04 管理用户身份和逻辑访问。	APO01.05	I&T 相关角色和职责的定义	用户账户和特权审查的结果	内部
	APO03.02	信息架构模型	获得批准的用户访问权限	内部

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
DSS05.05 管理对 I&T 资产的物理访问。	**自**	**描述**	**描述**	**至**
			访问日志	DSS06.03，MEA04.07
			获得批准的访问请求	内部
DSS05.06 管理敏感文档和输出设备。	APO03.02	信息架构模型	访问特权	内部
			敏感文档和设备的清单	内部
DSS05.07 管理漏洞并监控基础设施的安全相关事件。			安全事故单	DSS02.02
			安全事故特征	内部
			安全事件日志	内部
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
信息安全	Skills Framework for the Information Age，第 6 版，2015 年	SCTY
信息安全管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage— E.8. 信息安全管理
渗透测试	Skills Framework for the Information Age，第 6 版，2015 年	PENT
安全管理	Skills Framework for the Information Age，第 6 版，2015 年	SCAD

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
信息安全政策	制定对公司的信息及相关系统和基础设施的保护准则。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
营造安全和隐私的维护，人人有责的文化。	1) HITRUST CSF，第 9 版，2017 年 9 月；(2) ISF, The Standard of Good Practice for Information Security 2016	(1) 01.03 User Responsibilities; (2) PM2.1 Security Awareness Program

G. 组件：服务、基础设施和应用程序
• 目录服务 • 电子邮件过滤系统 • 身份和访问管理系统 • 安全意识服务 • 安全信息和事件管理 (SIEM) 工具 • 安全运营中心 (SOC) 服务 • 第三方安全评估服务 • URL 过滤系统

领域：交付、服务与支持 管理目标：DSS06 — 妥当管理的业务流程控制	焦点领域：COBIT 核心模型

描述

定义并维护合适的业务流程控制，确保与内部或外包业务流程相关或经过这些流程处理的信息满足所有相关信息控制要求。确定相关的信息控制要求。管理和执行适当的输入、吞吐量和输出控制（应用程序控制），确保信息和信息处理满足这些控制要求。

目的

维护企业内部业务流程或外包运营所处理的信息资产的完整性和安全性。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG05 以客户为中心的服务文化 • EG08 内部业务流程功能的优化 • EG12 妥当管理的数字化转型计划	AG08 通过集成应用程序和技术来推行和支持业务流程

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG08	a. 执行业务服务或流程的时间 b. 因技术集成问题而延迟或产生额外成本的 I&T 促成的业务计划的数量 c. 因技术集成问题需要延迟或返工的业务流程变更的数量 d. 独立运行和未集成的应用程序或关键基础设施的数量
EG05	a. 客户服务中断的次数 b. 业务利益相关方认为客户服务交付达到议定水平的百分比 c. 客户投诉的数量 d. 客户满意度调查结果的变化趋势		
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		
EG12	a. 在预算内按时交付的计划数量 b. 对计划交付满意的利益相关方的百分比 c. 中止的业务转型计划的百分比 d. 定期报告状态更新的业务转型计划的百分比		

A. 组件：流程

管理实践	指标示例
DSS06.01 调整业务流程中融入的控制活动，使其符合企业目标。 根据企业风险持续评估和监控业务流程活动及相关控制的执行情况，确保处理控制与业务需求保持一致。	a. 已列入完成清单的关键流程和关键控制的百分比 b. 与业务需求保持一致的处理控制的百分比

A. 组件：流程（续）	
活动	**能力级别**
1. 识别并记录关键业务流程所需的控制活动，以满足战略、运营、报告和合规性目标的控制要求。	2
2. 根据业务的固有风险确定控制活动的优先级。识别关键控制。	
3. 明确关键控制活动的所有权。	
4. 实施自动化控制。	3
5. 采用端到端的方式持续监控控制活动，以识别改进机会。	4
6. 持续改进业务流程控制的设计和运作。	5

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	3.1 Preparation (Task 10, 11)
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 14: Controlled Access Based on the Need to Know

管理实践	指标示例
DSS06.02 控制信息的处理。 基于企业风险操作业务流程活动和相关控制的执行。确保信息的处理有效、完整、准确、及时和安全（即反映经过授权的合法业务用途）。	a. 表明关键控制失败的事故和审计报告结果的数量 b. 测试计划中关键控制的覆盖百分比

活动	能力级别
1. 对交易的发起人进行身份认证，并验证其是否有权发起该交易。	2
2. 确保在交易的发起和审批方面实行适当的职责分离。	
3. 验证交易是否准确、完整和有效。控制的内容可能涵盖顺序、限制、范围、有效性、合理性、表格检查、存在性、键值验证、校验数字位、完整性、重复和逻辑关系检查，以及时间编辑。应定期审查和确认验证标准和参数。在尽可能接近发起交易的时间点验证输入数据并进行编辑，或在适用时发回进行校正。	3
4. 在不影响原始交易授权等级的情况下，更正输入错误的数据并重新提交。适当情况下重建交易，并将原始文件适当保留一段时间。	
5. 维护数据在整个处理周期中的完整性和有效性。确保检测错误交易不会中断有效交易的处理。	
6. 以授权的方式处理输出，将其发送给适当的接收者，并在传输期间保护相关信息。验证输出的准确性和完整性。	
7. 在业务处理发生意外中断时维护数据的完整性。在处理故障之后确认数据的完整性。	
8. 在内部应用程序和业务/操作职能部门（企业内部或外部）之间传递交易数据之前，应检查寻址是否正确、请求来源的真实性和内容的完整性。在传输或运输期间保持数据的真实性和完整性。	

相关指南（标准、框架、合规性要求）	详细参考
HITRUST CSF，第 9 版，2017 年 9 月	13.01 Openness and Transparency；13.02 Individual Choice and Participation
ISF, The Standard of Good Practice for Information Security 2016	BA1.4 Information Validation

A. 组件：流程（续）	
管理实践	**指标示例**
DSS06.03 管理角色、职责、访问特权和权限级别。 管理业务角色、职责、权限级别和必要的职责分离，为实现业务流程目标提供支持。授权访问与业务信息流程相关的所有信息资产，包括由业务、IT 和第三方保管的信息资产。这可以确保企业知道数据在何处以及谁在代表企业处理数据。	a. 由于访问或职责分离违规造成的事故和审计发现的数量 b. 已分配访问权限和权限级别的业务流程角色的百分比 c. 职责分离明确的业务流程角色的百分比

活动	能力级别
1. 根据核准的岗位职责说明和业务流程活动分配角色和职责。	2
2. 根据核准的工作角色分配权限级别，以审批交易、交易限制以及与业务流程相关的其他决策。	
3. 为敏感活动分配角色，以实行明确的职责分离。	
4. 根据预定义的工作角色以及执行工作活动所需的最低权限原则分配访问权限和特权。如果工作角色发生变更或员工离开业务流程区域，应立即删除或修改其相应的访问权限。定期审查，确保访问权限能够应对当前的威胁、风险、技术和业务需求。	3
5. 定期提供关于角色和职责的意识和培训，确保所有人了解自己的职责、控制的重要性，以及各种形式的公司信息的安全性、完整性、机密性和隐私性。	
6. 确保管理权限得到充分和有效的保护、跟踪和控制，以防被滥用。	
7. 定期审查访问控制的定义、日志和异常报告。确保所有访问权限都有效，并与当前员工及其分配的角色保持一致。	4

相关指南（标准、框架、合规性要求）	详细参考
HITRUST CSF，第 9 版，2017 年 9 月	13.04 Collection, Use and Disclosure
ISO/IEC 27002:2013/Cor.2:2015(E)	7. Human resource security
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 5: Controlled Use of Administrative Privileges

管理实践	指标示例
DSS06.04 管理错误和异常。 管理业务流程异常和错误，便于补救工作的进行，执行规定的纠偏行动并在必要时上报。这种对异常和错误处理的方式可以保证业务信息流程的准确性和完整性。	a. 数据输入不完整导致处理效率低下的频率 b. 及时检测到错误的次数 c. 得到有效补救的数据处理错误的数量

活动	能力级别
1. 审查错误、异常和偏差。	2
2. 跟进、纠正、批准并重新提交原始文件和交易。	
3. 保留补救措施的证据。	
4. 定义和维护相应的程序，以明确错误和异常的责任归属，纠正错误，覆盖错误以及处理失衡状况。	3
5. 及时报告相关业务信息流程错误，以执行实质原因和趋势分析。	4

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

A. 组件：流程（续）	
管理实践	**指标示例**
DSS06.05 确保信息事件的可追溯性和问责制。 确保业务信息可以追溯至原始的业务事件和可问责的各方。这种可发现性能够保证业务信息是可靠的，并且是按照定义的目标进行处理的。	a. 无法恢复交易历史记录的事故数量 b. 可追溯的交易日志的完整性百分比

活动	能力级别
1. 捕获源信息、支持性证据和交易记录。	2
2. 根据业务需求定义保留政策的要求，以满足运营、财务报告和合规性需求。	3
3. 根据保留政策处置源信息、支持性证据和交易记录。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
DSS06.06 保护信息资产的安全。 通过获批准的方法保护企业可访问的信息资产的安全，包括电子形式的信息（例如便携式介质设备、用户应用程序和存储设备，或其他创建任何形式的新资产的方法）、物理形式的信息（例如源文档或输出报告）以及传输中的信息。这通过对信息提供端到端的安全保护使企业受益。	a. 将敏感交易数据提供给错误接收者的案例数量 b. 关键数据完整性受损的频率

活动	能力级别
1. 根据其分类来限制信息的使用、分发和物理访问。	2
2. 提供关于适当用途的意识和培训。	
3. 运用数据分类、适当用途以及安全政策和程序来保护业务部门控制下的信息资产。	3
4. 识别并运用流程、工具和技术来合理地验证合规性。	
5. 向企业和其他利益相关方报告违规和偏差。	4

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	AC.MP Manage Access Permissions
The CIS Critical Security Controls for Effective Cyber Defense，第 6.1 版，2016 年 8 月	CSC 18: Application Software Security

B. 组件：组织结构									
关键管理实践	执行委员会	首席信息官	I&T 治理委员会	首席信息安全官	业务流程所有者	数据管理职能部门	服务经理	信息安全经理	法律顾问
DSS06.01 调整业务流程中融入的控制活动，使其符合企业目标。	R		A		R				
DSS06.02 控制信息的处理。		R	A	R	R	R			R
DSS06.03 管理角色、职责、访问特权和权限级别。		R	A	R	R			R	
DSS06.04 管理错误和异常。		R		R	A		R		
DSS06.05 确保信息事件的可追溯性和问责制。		R		R	A				
DSS06.06 保护信息资产的安全。		R		R	A				

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
DSS06.01 调整业务流程中融入的控制活动，使其符合企业目标。	APO01.07	• 数据分类准则 • 数据完整性程序	根本原因分析和建议	BAI06.01； MEA02.04； MEA04.04； MEA04.06； MEA04.07
			针对处理的有效性审查的结果	MEA02.04
DSS06.02 控制信息的处理。	BAI05.05	操作和使用计划	处理控制报告	内部
	BAI07.02	迁移计划		
DSS06.03 管理角色、职责、访问特权和权限级别。	APO11.01	质量管理系统 (QMS) 的角色、职责和决策权	分配的权限级别	APO01.05
	APO13.01	信息安全管理系统 (ISMS) 范围声明	分配的角色和职责	APO01.05
	DSS05.05	访问日志	分配的访问权限	APO07.04
	EDM04.02	分配的资源管理职责		

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	输入		输出	
DSS06.04 管理错误和异常。	自	描述	描述	至
			错误报告和根本原因分析	内部
			错误纠正和补救的证据	MEA02.04
DSS06.05 确保信息事件的可追溯性和问责制。			交易记录	内部
			保留要求	内部；APO14.09
DSS06.06 保护信息资产的安全。			违规报告	DSS05.03

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-37，修订版 2，2017 年 9 月	3.1 Preparation (Task 10, 11): Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
信息安全	Skills Framework for the Information Age，第 6 版，2015 年	SCTY
安全管理	Skills Framework for the Information Age，第 6 版，2015 年	SCAD

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
业务控制指南	定义业务流程控制，以确保适当的控制并减少舞弊行为和错误的风险。确定手动控制以保护文档（例如源文档、输入、处理和输出文档）；确定监督控制，以审查文件的流转并确保正确的处理。包括 I&T 一般控制（例如物理安全性、访问和身份认证，以及变更管理）和应用程序控制（例如编辑检查、系统配置和安全设置）。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
营造对业务流程实施合理控制重视的文化，将这些控制融入到开发的应用程序中，或在购买应用程序或作为服务访问应用程序时将这些控制作为一个必要的要求。培养所有员工的控制意识，以保护组织的所有资产（例如纸质记录和设施）。		

G. 组件：服务、基础设施和应用程序
• 自动化应用程序控制 • 事件日志审计工具

4.5 监控、评价和评估 (MEA)

01 妥当管理的绩效和一致性监控

02 妥当管理的内部控制系统

03 妥当管理的外部要求合规性

04 妥当管理的鉴证

领域：监控、评价和评估 管理目标：MEA01 — 妥当管理的绩效和一致性监控	焦点领域：COBIT 核心模型

描述

收集、验证和评价企业和一致性目标与指标。监控流程和实践是否正在按照协定的绩效和一致性目标及指标运行。提供及时的系统性报告。

目的

提供透明的绩效和一致性，并推动目标的实现。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG01 有竞争力的产品和服务的组合 • EG04 财务信息的质量 • EG07 管理信息的质量 • EG08 内部业务流程功能的优化	• AG05 提供符合业务需求的 I&T 服务 • AG10 I&T 管理信息的质量

企业目标的指标示例		一致性目标的指标示例	
EG01	a. 达到或超过收益和/或市场份额目标的产品和服务的百分比 b. 达到或超过客户满意度的产品和服务的百分比 c. 带来竞争优势的产品和服务的百分比 d. 新产品和服务的上市时间	AG05	a. 认为 I&T 服务交付达到议定服务水平的业务利益相关方的百分比 b. 因 I&T 服务事故造成业务中断的次数 c. 对 I&T 服务交付质量满意的用户的百分比
EG04	a. 有关企业财务信息的透明度、了解度和准确性的关键利益相关方满意度调查 b. 不遵守财务相关法规的成本	AG10	a. 考虑到可用资源，用户对 I&T 相关管理信息的质量、及时性和可用性的满意度水平 b. 主要因 I&T 相关信息错误或不可用导致的错误业务决策的比率和程度 c. 满足质量准则的信息的百分比
EG07	a. 董事会和执行管理层对决策信息的满意度 b. 基于不准确信息的错误业务决策所导致的事故数量 c. 为有效业务决策提供支持性信息所花的时间 d. 管理信息的及时性		
EG08	a. 董事会和执行管理层对业务流程能力的满意度 b. 客户对服务交付能力的满意度 c. 供应商对供应链能力的满意度		

A. 组件：流程

管理实践	指标示例
MEA01.01 制定监控方法。 与利益相关方一起制定和维护监控方法，以定义用于衡量业务解决方案、服务交付情况以及有助于实现企业目标的对象、范围和方法。将此方法与公司绩效管理制度整合在一起。	a. 定义了目标和指标的流程的百分比 b. 在公司绩效管理系统中整合了监控方法的百分比

A. 组件：流程（续）	
活动	**能力级别**
1. 识别利益相关方（例如管理层、流程所有者和用户）。	2
2. 与利益相关方合作，使用通用定义（例如业务术语表、元数据和分类法）、基准指标和基准检测来沟通企业对监控、汇总和报告的要求和目标。	
3. 调整并持续维护监控和评估方法，使其与企业用于收集数据和报告的方法和工具（例如业务智能应用程序）保持一致。	
4. 就目标和指标的类型（例如一致性、绩效、价值、风险）、分类（目标与指标之间的分类和关系）以及数据（证据）保留达成共识。	
5. 申请、分配用于监控的资源并排定其优先级，同时考虑适当性、效率、有效性和机密性。	
6. 定期验证所使用的方法，并识别新的或变更的利益相关方、要求和资源。	3
7. 对监控与报告的生命周期管理和变更控制流程达成共识，包括报告、指标、方法、基准指标和基准检测的改进机会。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Supporting Processes - Measurement and Analysis
SF, The Standard of Good Practice for Information Security 2016	SI2 Security Performance
ISO/IEC 27001:2013/Cor.2:2015(E)	9.1 Monitoring, measurement, analysis and evaluation
ISO/IEC 27004:2016(E)	6. Characteristics; 7. Types of measures; 8. Processes
ISO/IEC 38500:2015(E)	5.5 Principle 4: Performance; 5.6 Principle 5: Conformance
美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	3.1 Preparation (Task 13); 3.3 Selection (Task 2); 3.7 Monitoring (Task 1)
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.4 Assessment, authorization and monitoring (CA-2, CA-7); 3.20 System and information integrity (SI-4)

管理实践	指标示例
MEA01.02 设定绩效和一致性目标。 在绩效衡量系统内与利益相关方合作，定义、定期审查、更新和批准绩效和一致性目标。	a. 获得利益相关方批准的目标和指标的百分比 b. 目标和指标的有效性得到审查和改进的流程的百分比

活动	能力级别
1. 定义目标和指标。定期与利益相关方一起审查，以识别任何重大的缺失项并确定目标和容忍度的合理性。	2
2. 评估目标和指标是否具备足够的明确性、可衡量性、可实现性、相关性和时限性 (SMART)。	
3. 与关键的尽职调查利益相关方（例如法律、审计、人力资源、道德、合规、财务）沟通对绩效和一致性目标及容忍度（与指标相关）的建议变更。	
4. 向此信息的用户发布变更后的目标和容忍度。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Supporting Processes - Process Management
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.4 Assessment, authorization and monitoring (CA-5)

管理实践	指标示例
MEA01.03 收集并处理绩效和一致性数据。 及时收集并处理符合企业方针的准确数据。	a. 受到监控的关键流程的百分比 b. 为满足组织目标而受到监控、基准检测和改进的控制环境的百分比

A. 组件：流程（续）	
活动	**能力级别**
1. 收集来自既定流程的数据（可能的话采用自动方式收集）。	2
2. 评估所收集的数据的效率（与提供洞察力相关的工作量）和适当性（有用性和意义），并验证数据的完整性（准确性和完整性）。	
3. 汇总数据以支持对商定指标的衡量。	
4. 调整汇总的数据，使其与企业的报告方法和目标保持一致。	3
5. 使用合适的工具和系统进行数据处理和分析。	4
相关指南（标准、框架、合规性要求）	**详细参考**
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.20 System and information integrity (SI-2)
管理实践	**指标示例**
MEA01.04 分析和报告绩效。 对照目标定期审查和报告绩效。使用一种能提供简洁而全面的 I&T 绩效视图并且适应企业监控系统的方法。	a. 与企业监控系统保持一致的目标和指标的百分比 b. 按计划交付的绩效报告的百分比 c. 输出保证符合目标且在容忍度范围内的流程的百分比
活动	**能力级别**
1. 设计简洁、易于理解且适合各种管理需求和受众的流程绩效报告。促进及时和有效的决策（如记分卡、交通信号灯报告）。确保以可理解的方式沟通目标与指标之间的因果关系。	3
2. 将报告分发给相关的利益相关方。	
3. 分析偏离目标的原因，采取补救措施，分配负责补救的责任，以及跟进。在适当的时间审查所有偏差，必要时寻找根本原因。记录问题，以便在问题重新出现时提供进一步指导。记录结果。	4
4. 在可行的情况下，将绩效和合规性纳入员工的个人绩效目标，并将绩效目标的实现与组织的奖励薪酬制度联系起来。	
5. 将绩效值与内部目标和基准指标进行比较，并在可能的情况下与外部基准指标（行业和主要竞争对手）进行比较。	
6. 分析绩效与合规性趋势并采取适当措施。	
7. 适当时提出目标和指标的变更建议。	5
相关指南（标准、框架、合规性要求）	**详细参考**
CMMI 数据管理成熟度模型，2014 年	Supporting Processes - Measurement and Analysis
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.3 Audit and accountability (AU-6)
管理实践	**指标示例**
MEA01.05 确保实施纠正措施。 协助利益相关方识别、发起和跟踪纠正措施来处理异常。	a. 重复出现的异常的数量 b. 已执行的纠正措施的数量
活动	**能力级别**
1. 审查管理层的响应措施、方案和建议，以解决问题和重大偏差。	2
2. 确保纠正措施的责任分配得到维护。	
3. 跟踪已承诺的行动的结果。	
4. 向利益相关方报告结果。	
相关指南（标准、框架、合规性要求）	**详细参考**
ITIL 第 3 版，2011 年	Continual Service Improvement, 4.1 The 7-Step Improvement Process
美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	3.7 Monitoring (Task 3)
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.3 Audit and accountability (AU-5)

B. 组件：组织结构												
关键管理实践	执行委员会	首席执行官	首席财务官	首席运营官	首席信息官	I&T 治理委员会	业务流程所有者	关系经理	开发总监	IT 运营总监	服务经理
MEA01.01 制定监控方法。	R	A	R	R	R	R					
MEA01.02 设定绩效和一致性目标。	A						R	R	R	R	R
MEA01.03 收集并处理绩效和一致性数据。					A		R	R	R	R	R
MEA01.04 分析和报告绩效。					A		R	R	R	R	R
MEA01.05 确保实施纠正措施。					A		R	R	R	R	R

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
MEA01.01 制定监控方法。	EDM05.01	• 企业报告要求的评估 • 报告和沟通原则	获得批准的监控目标和指标	内部
			监控要求	内部
	EDM05.02	验证和批准强制性报告的规则		
	EDM05.03	报告有效性的评估		
MEA01.02 设定绩效和一致性目标。	APO01.11	流程改进跟踪的绩效目标和指标	监控目标	所有 APO； 所有 BAI； 所有 DSS； 所有 MEA

C. 组件：信息流和信息项（另请参阅第 3.6 节）（续）				
管理实践	输入		输出	
MEA01.03 收集并处理绩效和一致性数据。	自	描述	描述	至
	APO01.11	流程能力评估	已处理的监控数据	内部
	APO05.03	投资组合绩效报告		
	APO09.04	服务水平绩效报告		
	APO10.05	供应商合规性监控审查的结果		
	BAI01.06	计划绩效审查的结果		
	BAI04.04	可用性、性能和容量监控审查报告		
	BAI05.05	成功衡量指标和结果		
	DSS01.05	设施评估报告		
	DSS02.07	• 事故状态和趋势报告 • 请求履行状态和趋势报告		
MEA01.04 分析和报告绩效。			绩效报告	所有 APO； 所有 BAI； 所有 DSS； 所有 MEA； EDM01.03
MEA01.05 确保实施纠正措施。	APO01.09	违规补救措施	补救措施和任务	所有 APO； 所有 BAI； 所有 DSS； 所有 MEA
	EDM05.02	上报指南	行动的状态和结果	EDM01.03
相关指南（标准、框架、合规性要求）		详细参考		
美国国家标准与技术研究所特别出版物 800-37，修订版 2，2017 年 9 月		3.1 Preparation (Task 13): Inputs and Outputs; 3.3 Selection (Task 2): Inputsand Outputs; 3.7 Monitoring (Task 1, Task 3): Inputs and Outputs		

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
一致性审查	Skills Framework for the Information Age，第 6 版，2015 年	CORE
ICT 质量管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage—E.6. ICT Quality Management
质量保证	Skills Framework for the Information Age，第 6 版，2015 年	QUAS

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
自我评估政策	为管理层提供运营评估职责方面的指导，作为持续改进计划的一部分。通常用于根据业务需求向企业内部的高管或董事会报告当前的能力、进度和改进情况。可在流程改进计划期间或之后（即在完成改进之后评估进展）进行评估。		
举报政策	鼓励员工大胆地提出问题和质疑。确保员工能够收到回复；如果他们对回复不满意，可以将问题上报。确保为提出问题的员工提供保护，使他们不必担心遭到报复。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
营造持续改进业务和 I&T 流程的文化，以实现组织目标和优化绩效。		

G. 组件：服务、基础设施和应用程序
• 绩效衡量系统（例如平衡计分卡、技能管理工具） • 自我评估工具

领域：监控、评价和评估 管理目标：MEA02 — 妥当管理的内部控制系统	焦点领域：COBIT 核心模型

描述

持续监控和评估控制环境，包括自我评估和自我意识。使管理层能识别控制缺陷和低效率的情况并发起改进行动。计划、组织和维护适用于内部控制评估和流程控制有效性的标准。

目的

在内部控制系统的充分性方面实现关键利益相关方透明度，从而建立运营信任、对实现企业目标的信心并充分了解剩余风险。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG03 遵守外部法律和法规 • EG11 遵守内部政策	AG11 I&T 遵守内部政策
企业目标的指标示例	**一致性目标的指标示例**
EG03 a. 不合规的成本，包括结算和罚款 b. 引起负面舆论或负面影响的不合规问题的数量 c. 监管机构指出的违规问题的数量 d. 与业务伙伴合同协议有关的不合规问题的数量	AG11 a. 与违反 I&T 相关政策有关的事故的数量 b. 内部政策的例外情况的数量 c. 政策审查和更新的频率
EG11 a. 与违反政策有关的事故的数量 b. 了解政策的利益相关方的百分比 c 得到有效标准和工作实践支持的政策的百分比	

A. 组件：流程

管理实践	指标示例
MEA02.01 监控内部控制。 持续监控、改进 I&T 控制环境和控制框架并检测其基准指标，以满足组织的目标。	a. 重大的内部控制违规的数量 b. 为满足组织目标而受到持续监控、基准检测和改进的控制环境和框架的百分比

活动	能力级别
1. 识别内部控制系统的边界，例如，考虑组织内部控制如何将外包和/或离岸开发或生产活动纳入考虑范围。	3
2. 评估外部服务提供商的内部控制状态。确认服务提供商遵守法律和监管要求以及合同义务。	
3. 根据组织治理标准和业内接受的框架与实践，执行内部控制监控和评估活动，包括监控和评估管理层监督活动的效率和有效性。	
4. 确保及时报告、跟踪和分析控制异常，并根据风险管理概况按优先级实施适当的纠正措施（例如，将某些异常归类为关键风险，其他异常归类为非关键风险）。	
5. 考虑对内部控制系统进行独立评估（例如内部审计或同行评审）。	
6. 考虑不断变化的业务和 I&T 风险、组织控制环境以及相关的业务和 I&T 流程，维护内部控制系统。如存在差距，应评估并提出变更建议。	4
7. 根据业内认可的标准和良好实践进行基准检测，以定期评估控制框架的性能。考虑正式采用持续改进方法进行内部控制监控。	5

A. 组件：流程（续）	
相关指南（标准、框架、合规性要求）	**详细参考**
HITRUST CSF，第 9 版，2017 年 9 月	09.10 Monitoring
ISO/IEC 38502:2017(E)	5.5 Governance and internal control
美国国家标准与技术研究所特别出版物 800-53，修订版 5（草稿），2017 年 8 月	3.3 Audit and accountability (AU-2)
管理实践	**指标示例**
MEA02.02 审查业务流程控制的有效性。 审查控制措施的运行情况，包括监控和测试证据，以确保业务流程中的控制措施有效运行。通过定期测试、持续监测、独立评估、建立指挥控制中心和网络运行中心等机制来维护证明控制措施有效运行的证据。这些证据可保证企业控制满足与业务、监管和社会责任相关的要求。	a. 外部资质和认证报告识别的漏洞的数量 b. 为确保业务流程中的控制有效运行而受到监控和测试的控制的数量

活动	能力级别
1. 了解组织目标的风险并排定优先级。	3
2. 确定关键控制并制定合适的策略来验证控制。	
3. 确定能够指示内部控制环境是否有效运行的信息。	
4. 维护控制有效性的证据。	4
5. 制定并实施具有成本效益的程序，以根据适用的信息质量标准获取此信息。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	
管理实践	**指标示例**
MEA02.03 执行控制自我评估。 鼓励管理层和流程所有者通过持续的自我评估计划来评估管理层对流程、政策及合同的控制完整性和有效性，从而积极改进控制。	a. 已执行的自我评估的数量 b. 通过自我评估识别的与行业标准或良好实践之间存在的差距的数量

活动	能力级别
1. 定义并商定一致的方法来执行控制自我评估以及协调内部与外部的审计师。	3
2. 维护评估计划和范围，并确定进行自我评估的评估标准。制定沟通计划，向业务、IT 和一般管理层以及董事会沟通自我评估流程的结果。在设计自我评估时考虑内部审计标准。	
3. 考虑持续监控的总体有效性和效率，确定定期进行自我评估的频率。	
4. 将自我评估的职责分配给合适的人员，以确保客观性和能力。	
5. 进行独立审查，以确保自我评估的客观性并借鉴其他企业的内部控制良好实践。	
6. 将自我评估的结果与行业标准和良好实践进行比较。	4
7. 总结并报告自我评估和基准检测的结果，以采取补救措施。	5

相关指南（标准、框架、合规性要求）	详细参考
ISO/IEC 27001:2013/Cor.2:2015(E)	9.3 Management review
美国国家标准与技术研究所特别出版物 800-37，修订版 2（草稿），2018 年 5 月	3.7 Monitoring (Task 2)

A. 组件：流程（续）	
管理实践	**指标示例**
MEA02.04 识别和报告控制缺陷。 识别控制缺陷并分析和确定其根本原因。将控制缺陷上报给利益相关方。	a. 从发生内部控制缺陷到报告的时间 b. 从识别异常到完成商定行动的时间 c. 来自控制评估的补救措施得到实施的百分比

活动	能力级别
1. 向流程所有者和 I&T 利益相关方沟通控制异常上报、根本原因分析以及报告的程序。	3
2. 考虑相关的企业风险，以确定控制异常和故障的上报阈值。	
3. 识别、报告并记录控制异常。分配解决这些异常的职责并报告状态。	
4. 确定哪些控制异常应传达到负责该职能的个人，以及哪些异常应上报。通知受影响的流程所有者和利益相关方。	
5. 跟进所有异常情况，确保商定的行动得到执行。	4
6. 识别、启动、跟踪和实施来自控制评估和报告的补救措施。	5

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

B. 组件：组织结构															
关键管理实践	**首席财务官**	**首席风险官**	**首席信息官**	**首席技术官**	**I&T 治理委员会**	**业务流程所有者**	**项目管理办公室**	**开发总监**	**IT 运营总监**	**IT 行政总监**	**服务经理**	**信息安全经理**	**业务连续性经理**	**隐私官**
MEA02.01 监控内部控制。		R	A	R		R	R	R	R	R	R	R	R	R
MEA02.02 审查业务流程控制的有效性。	R		A	R	R	R								
MEA02.03 执行控制自我评估。		R	A	R		R	R	R	R	R	R	R	R	R
MEA02.04 识别和报告控制缺陷。			A	R		R	R	R	R	R	R	R	R	R

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
MEA02.01 监控内部控制。	APO12.04	第三方风险评估的结果	基准检测和其他评估的结果	所有 APO；所有 BAI；所有 DSS；所有 MEA；EDM01.03
	APO13.03	信息安全管理系统 (ISMS) 审计报告	内部控制的监控和审查结果	所有 APO；所有 BAI；所有 DSS；所有 MEA；EDM01.03
	在 COBIT 外部	行业标准和良好实践		
MEA02.02 审查业务流程控制的有效性。	BAI05.06	合规性审计结果	控制有效性的证据	内部
	BAI05.07	操作使用情况的审查		
MEA02.03 执行控制自我评估。			自我评估计划和衡量标准	所有 APO；所有 BAI；所有 DSS；所有 MEA
			自我评估审查的结果	所有 APO；所有 BAI；所有 DSS；所有 MEA；EDM01.03
			自我评估的结果	内部
MEA02.04 识别和报告控制缺陷。	APO11.03	未能提供高品质的根本原因	补救措施	所有 APO；所有 BAI；所有 DSS；所有 MEA
	APO12.06	风险相关的根本原因	控制缺陷	所有 APO；所有 BAI；所有 DSS；所有 MEA
	DSS06.01	• 针对处理的有效性审查的结果 • 根本原因分析和建议		
	DSS06.04	错误纠正和补救的证据		

相关指南（标准、框架、合规性要求）	详细参考
美国国家标准与技术研究所特别出版物 800-37，修订版 2，2017 年 9 月	3.7 Monitoring (Task 2): Inputs and Outputs

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
风险管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage—E.3. Risk Management

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
内部控制政策	沟通管理层的内部控制目标。建立企业内部控制系统的设计和运作标准，以减少所有风险敞口。为持续监控和评估控制环境提供指导，包括自我意识和自我评估。		
内部控制自我评估指南	建议持续监控内部控制，以识别有效性方面存在的缺陷和差距及确定其根本原因，然后启动行动计划和纠正里程碑计划，以报告给利益相关方。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
提高对有效控制环境的重要性的认识。鼓励积极主动的风险意识和自我意识文化，包括进行自我评估和独立鉴证审查的承诺。		

G. 组件：服务、基础设施和应用程序
• COBIT 和相关产品/工具 • 第三方内部控制评估服务

领域：监控、评价和评估 管理目标：MEA03 — 妥当管理的外部要求合规性	焦点领域：COBIT 核心模型

描述

评估 I&T 流程和 I&T 支持的业务流程是否符合法律、法规和合同要求。确保已识别并符合这些要求，并将 IT 合规性与整体企业合规性进行整合。

目的

确保企业符合所有适用的外部要求。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标		一致性目标
EG03 遵守外部法律和法规	→	AG01 I&T 合规且支持业务遵守外部法律和法规
企业目标的指标示例		**一致性目标的指标示例**
EG03 a. 不合规的成本，包括结算和罚款 b. 引起负面舆论或负面影响的不合规问题的数量 c. 监管机构指出的违规问题的数量 d. 与业务伙伴合同协议有关的不合规问题的数量		AG01 a. IT 不合规的成本，包括费用结算和罚款，以及声誉损失造成的影响 b. 向董事会报告或者引起舆论或难堪的 IT 相关不合规问题的数量 c. 与 IT 服务提供商的合同协议有关的不合规问题的数量

A. 组件：流程

管理实践	指标示例
MEA03.01 识别外部合规要求。 持续监控当地和国际法律、法规以及其他外部要求的变化，并从 I&T 角度来识别合规性要求。	a. 合规性要求审查的频率 b. 关键利益相关方对就监管审查的合规性流程感到满意的百分比

活动	能力级别
1. 分配责任，以识别和监控与企业的业务和 IT 运营中的 IT 资源使用及信息处理相关的法律、法规和其他外部合同要求的任何变更。	2
2. 识别和评估所有潜在的合规性要求以及对数据流、隐私、内部控制、财务报告、行业特定法规、知识产权、健康和安全等领域的 I&T 活动的影响。	
3. 评估 I&T 相关的法律和监管要求对与 IT 运营、服务提供商和贸易合作伙伴相关的第三方合同的影响。	
4. 定义不合规的后果。	
5. 适当情况下，聘请独立法律顾问来指导法律、法规和标准的变更。	3
6. 维护一份针对所有相关法律、法规和合同要求及其影响和必要行动的最新记录。	
7. 维护一份关于企业外部合规性要求的统一和整合的总体登记表。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	BC.RR Determine Legal / Regulatory Requirements
HITRUST CSF，第 9 版，2017 年 9 月	06.01 Compliance with Legal Requirements
ISF, The Standard of Good Practice for Information Security 2016	SM2.3 Legal and Regulatory Compliance

A. 组件：流程（续）	
管理实践	**指标示例**
MEA03.02 优化对外部要求的响应。 审查和调整政策、原则、标准、程序和方法论，来确保已经满足和传达法律、法规和合同要求。考虑采用和调整行业标准、良好实践行为规范和良好实践指南。	a. 从识别外部合规性问题到解决问题的平均时间 b. 相关人员对关于新的和变更后的监管合规性要求的沟通感到满意的百分比

活动	能力级别
1. 定期审查和调整政策、原则、标准、程序和方法，以确保它们有效满足必要的合规性要求并解决企业风险。必要时请内部和外部专家提供指导。	3
2. 向所有相关人员沟通新的和变更后的要求。	

相关指南（标准、框架、合规性要求）	详细参考
King IV Report on Corporate Governance for South Africa，2016 年	Part 5.4: Governance functional areas - Principle 13

管理实践	指标示例
MEA03.03 确认外部合规性。 确认政策、原则、标准、程序和方法符合法律、法规以及合同要求。	a. 每年识别的严重违规问题的数量 b. 流程所有者签字确认合规性的百分比

活动	能力级别
1. 定期评估企业所有职能部门的组织政策、标准、程序和方法，以确保遵守与信息处理相关的法律和监管要求。	3
2. 及时解决政策、标准和程序中的合规性差距。	
3. 定期评估业务和 IT 流程和活动，以确保遵守适用的法律、法规和合同要求。	
4. 定期审查反复出现的不合规的模式，并评估经验教训。	4
5. 根据审查结果和经验教训改进政策、标准、程序、方法以及相关的流程和活动。	5

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
MEA03.04 获得外部合规性鉴证。 获得并报告符合及遵守政策、原则、标准、程序和方法的保证。确认用于解决合规性问题的纠正措施及时结束。	a. 获取的合规性报告的数量 b. 根据独立审查确定合规的服务提供商的百分比 c. 从识别合规性差距到采取纠正措施的时间 d. 关于及时解决的合规性差距的纠正措施报告的数量

活动	能力级别
1. 定期确认业务和 IT 流程所有者及部门负责人是否遵守内部政策。	2
2. 定期开展内部和外部审查（以及适当时进行独立审查），以评估合规水平。	
3. 必要时，向第三方 I&T 服务提供商求证其对适用法律和法规的合规性水平。	
4. 必要时，向业务伙伴求证其对与公司间电子交易相关的适用法律和法规的合规性水平。	
5. 在企业层面整合关于法律、法规和合同要求且涵盖所有业务部门的报告。	3
6. 监控和报告不合规问题，并在必要时调查根本原因。	4

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Supporting Processes - Process Quality Assurance
ISO/IEC 27002:2013/Cor.2:2015(E)	18. 合规性

B. 组件：组织结构																	
关键管理实践	首席执行官	首席财务官	首席运营官	首席信息官	I&T 治理委员会	业务流程所有者	项目管理办公室	开发总监	IT 运营总监	IT 行政总监	服务经理	信息安全经理	业务连续性经理	隐私官	法律顾问	合规性	审计
MEA03.01 识别外部合规要求。				R		R								R	R	A	R
MEA03.02 优化对外部要求的响应。	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	A
MEA03.03 确认外部合规性。	R	R	R	R	R	R								R	R	A	
MEA03.04 获得外部合规性鉴证。				R											R	A	

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
	自	描述	描述	至
MEA03.01 识别外部合规要求。	在 COBIT 外部	法律和法规合规性要求	所需的合规性措施的日志	内部
			合规性要求登记表	内部
MEA03.02 优化对外部要求的响应。			沟通变更的合规性要求	所有 APO；所有 BAI；所有 DSS；所有 MEA；EDM01.01
			更新的政策、原则、程序和标准	APO01.09；APO01.11
MEA03.03 确认外部合规性。	BAI05.06	合规性审计结果	合规性确认	EDM01.03
	BAI09.05	已安装许可证的审计结果	已识别的合规性差距	MEA04.08
	BAI10.05	许可证偏差		
	DSS01.04	保单报告		
MEA03.04 获得外部合规性鉴证。	EDM05.02	验证和批准强制性报告的规则	合规性鉴证报告	EDM01.03
	EDM05.03	报告有效性的评估	不合规问题和根本原因的报告	EDM01.03；MEA04.04

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

D. 组件：人员、技能和胜任能力		
技能	相关指南（标准、框架、合规性要求）	详细参考
信息安全	Skills Framework for the Information Age，第 6 版，2015 年	SCTY

E. 组件：政策和程序			
相关政策	政策描述	相关指南	详细参考
合规性政策	确定法规、合同和内部合规性要求。说明评估符合法规、合同和内部要求的流程。列出流程中不同活动的角色和职责，并提供衡量合规性指标的指导。获得合规报告并确认合规性或纠正措施，以及时弥补合规性差距。		

F. 组件：文化、道德和行为		
关键文化元素	相关指南	详细参考
促进合规意识文化，包括对违反法律和监管要求的零容忍。		

G. 组件：服务、基础设施和应用程序
• 监管监测服务 • 第三方合规性评估服务

领域：监控、评价和评估 管理目标：MEA04 — 妥当管理的鉴证	焦点领域：COBIT 核心模型

描述

规划、确定范围并执行鉴证机制，以符合内部要求以及法律、法规和战略目标。执行独立的鉴证审查和活动，使管理层能够在企业中提供充分和可持续的鉴证。

目的

促使组织设计和制定高效和有效的鉴证机制，并使用基于公认的鉴证方法的路线图来指导鉴证审查的规划、范围界定、执行和后续跟进。

管理目标支持一系列主要的企业目标和一致性目标的实现：

企业目标	一致性目标
• EG03 遵守外部法律和法规 • EG11 遵守内部政策	AG11 I&T 遵守内部政策
企业目标的指标示例	**一致性目标的指标示例**
EG03 a. 不合规的成本，包括结算和罚款 b. 引起负面舆论或负面影响的不合规问题的数量 c. 监管机构指出的违规问题的数量 d. 与业务伙伴合同协议有关的不合规问题的数量	AG11 a. 与违反 I&T 相关政策有关的事故的数量 b. 内部政策的例外情况的数量 c. 政策审查和更新的频率
EG11 a. 与违反政策有关的事故的数量 b. 了解政策的利益相关方的百分比 c 得到有效标准和工作实践支持的政策的百分比	

A. 组件：流程

管理实践	指标示例
MEA04.01 确保鉴证提供商是独立的并且具有资质。 确保执行鉴证的实体是职能部门、业务群或组织范围之外的独立实体。执行鉴证的实体应表现出适当的态度和面貌，具备执行鉴证所需的技能和知识，并且遵守道德规范和专业标准。	a. 接受独立审查的流程的百分比 b. 服务提供商符合资质和能力要求的百分比

活动	能力级别
1. 遵守适用的道德规范和标准（例如 ISACA 职业道德规范）和（行业和区域特定的）鉴证标准（例如 ISACA IT 审计鉴证标准和国际审计与鉴证准则理事会 [IAASB] 的《国际鉴证业务框架》[IAASB 鉴证框架]）。	2
2. 确保鉴证提供商的独立性。	
3. 确保鉴证提供商的能力和资质。	

相关指南（标准、框架、合规性要求）	详细参考
HITRUST CSF，第 9 版，2017 年 9 月	06.03 Information System Audit Considerations

A. 组件：流程（续）	
管理实践	**指标示例**
MEA04.02 制定基于风险的鉴证机制计划。 根据内部和外部环境和背景的评估、无法实现企业目标的风险，以及实现相同目标的机会，在此基础之上确定鉴证目标。	a. 遵循获得批准的鉴证计划和计划标准的鉴证机制的百分比 b. 基于风险的鉴证计划机制的百分比

活动	能力级别
1. 了解企业战略和优先级。	2
2. 了解企业的内部环境。这种理解将有助于鉴证专业人员更好地评估企业目标以及企业目标和一致性目标的相对重要性，以及对这些目标而言最重要的威胁。反过来，这有助于为鉴证业务确定更好和更相关的范围。	
3. 了解企业的外部环境。这种理解将有助于鉴证专业人员更好地了解企业目标以及企业目标和一致性目标的相对重要性，以及对这些目标而言最重要的威胁。反过来，这有助于为鉴证业务确定更好和更相关的范围。	
4. 制定鉴证机制的年度总计划，包含汇总的鉴证目标。	3

相关指南（标准、框架、合规性要求）	详细参考
King IV Report on Corporate Governance for South Africa，2016 年	Part 5.4: Governance functional areas—Principle 15

管理实践	指标示例
MEA04.03 确定鉴证机制的目标。 定义鉴证机制的目标并与所有利益相关方达成共识。	a. 通过鉴证机制达成的目标的百分比 b. 利益相关方对鉴证机制目标感到满意的百分比

活动	能力级别
1. 确定鉴证机制的利益相关方及其利益，以确定鉴证机制的鉴证目标。	2
2. 就鉴证业务的高层次目标和组织界限达成共识。	
3. 考虑使用 COBIT 目标级联及其不同的级别来表达鉴证目标。	3
4. 确保鉴证业务的目标考虑到所有三个价值目标的组成部分：实现支持战略目标的效益；优化未实现战略目标的风险；以及优化实现战略目标所需的资源水平。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI 数据管理成熟度模型，2014 年	Supporting Processes - Process Quality Assurance

管理实践	指标示例
MEA04.04 定义鉴证机制的范围。 根据鉴证目标定义鉴证机制的范围并与所有利益相关方达成共识。	a. 基于范围并考虑到要收集的信息和要访谈的利益相关方的业务计划的数量 b. 利益相关方对基于鉴证目标的鉴证机制范围感到满意的百分比

活动	能力级别
1. 定义审查范围内的所有治理组件，即原则、政策和框架；流程；组织结构；文化、道德和行为；信息；服务、基础设施和应用程序；以及人员、技能和胜任能力	2
2. 考虑要收集的信息和要访谈的利益相关方，根据范围定义来制定业务计划。	3
3. 根据对企业架构的理解，确认并优化范围。	
4. 根据可用资源，优化鉴证业务的范围。	

相关指南（标准、框架、合规性要求）	详细参考
CMMI Cybermaturity Platform，2018 年	TP.LA Apply Logging and Audit Processes

A. 组件：流程（续）	
管理实践	**指标示例**
MEA04.05 定义鉴证机制的工作计划。 根据范围内的管理目标和治理组件，制定具体的鉴证机制的工作计划。	a. 被确认为效果较弱且缺乏用于减少剩余风险的既定实践的管理控制的百分比 b. 已审查的控制的数量 c. 利益相关方对鉴证机制的工作计划感到满意的百分比

活动	能力级别
1. 定义从范围内的管理控制收集和评估信息的详细步骤。重点评估与控制设计有关的良好实践的定义和应用，以及与控制有效性有关的控制目标的实现。	2
2. 了解管理目标的背景以及实施的辅助性管理控制。了解这些管理控制如何促进一致性目标和企业目标的实现。	
3. 了解所有利益相关方及其利益。	
4. 就期望的管理控制良好实践达成共识。	3
5. 如果管理控制较弱，应定义实践来识别剩余风险（为报告做准备）。	
6. 了解管理控制的生命周期阶段并就预期价值达成共识。	

相关指南（标准、框架、合规性要求）	详细参考
本管理实践没有相关指南	

管理实践	指标示例
MEA04.06 执行鉴证机制，重点关注设计有效性。 执行计划的鉴证机制。验证并确认落实的内部控制设计。此外还应考虑治理组件设计的成本效益，特别是在内部审计任务分配方面。	a. 考虑了设计成本效益的鉴证机制的百分比 b. 利益相关方对鉴证机制的设计感到满意的百分比

活动	能力级别
1. 优化对 IT 鉴证主题的理解。	2
2. 优化 IT 鉴证主题的范围。	
3. 观察/检查和审查管理控制方法。与控制所有者一起验证设计的完整性、相关性、及时性和可衡量性。	3
4. 询问控制所有者是否已分配治理组件的职责和总体责任。确认回复。测试职责和责任是否得到理解和接受。验证是否具备合适的技能和必要的资源。	
5. 重新考虑预防与检测和纠正类型的管理控制活动的平衡。	
6. 考虑为维护管理控制花费的精力和相关的成本/效益。	

相关指南（标准、框架、合规性要求）	详细参考
ISF, The Standard of Good Practice for Information Security 2016	SI1 Security Audit
ISO/IEC 27001:2013/Cor.2:2015(E)	9.2 Internal audit

管理实践	指标示例
MEA04.07 执行鉴证机制，重点关注运作有效性。 执行计划的鉴证机制。测试内部控制是否适当和充分。测试鉴证机制范围内的关键管理目标的成果。	a. 测试了范围内关键管理目标的成果的鉴证机制的百分比 b. 利益相关方对鉴证机制的执行感到满意的百分比

A. 组件：流程（续）	
活动	**能力级别**
1. 评估是否实现了范围内每个管理控制的预期成果，即评估管理控制的有效性（控制有效性）。	3
2. 通过寻找对管理控制目标产生影响的直接和间接证据，确保鉴证专业人员测试管理控制的成果或有效性。这意味着能够直接和间接地证实管理目标对一致性目标产生了可衡量的贡献，从而记录真正实现预期结果的直接和间接证据。	
3. 确定鉴证专业人员是否通过应用一系列测试技术来获得特定项/期间的直接或间接证据，以确保审查中的管理控制正在有效运作。确保鉴证专业人员还对管理控制结果的充分性进行了限制性审查，并确定要鉴证管理控制的性能是否充分，所需的实质性测试水平和额外工作。	
4. 调查是否可以通过优化步骤或寻求与其他管理控制的协同作用，来提高管理控制的效率和管理控制设计的有效性。	
相关指南（标准、框架、合规性要求）	**详细参考**
ISF, The Standard of Good Practice for Information Security 2016	SI1 Security Audit
SO/IEC 27001:2013/Cor.2:2015(E)	9.2 Internal audit
管理实践	**指标示例**
MEA04.08 报告和跟进鉴证机制。 在适当的情况下提供积极的鉴证意见，并提供与确定的运营绩效、外部合规性和内部控制弱点相关的改进建议。	a. 利益相关方接受鉴证报告 b. 利益相关方接受与确定的运营绩效、外部合规性和内部控制弱点相关的改进建议
活动	**能力级别**
1. 记录控制弱点的影响。	2
2. 在执行计划期间与管理层沟通，以便清楚地了解所执行的工作，并商定和接受初步发现和建议。	
3. 为管理层提供报告（与职权范围、范围和商定的报告标准保持一致），以支持举措的成果并明确对关键问题和重要行动的关注。	3
4. 监督鉴证活动，确保所执行的工作完整、符合目标且达到了可接受的质量水平。如果存在质量差距，应修改方法或详细步骤。	4
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	
管理实践	**指标示例**
MEA04.09 跟进建议和行动。 商定、跟进并实施已确定的改进建议。	a. 重复出现的弱点的数量 b. 已解决的弱点的数量
活动	**能力级别**
1. 商定并在组织内部实施必要的行动，以解决已确定的弱点和差距。	2
2. 在组织内部进行跟进，以确定是否采取了纠正措施并解决了内部控制弱点。	
相关指南（标准、框架、合规性要求）	**详细参考**
本管理实践没有相关指南	

B. 组件：组织结构													
关键管理实践	首席运营官	首席风险官	首席信息官	首席技术官	企业风险委员会	业务流程所有者	数据管理职能部门	IT 运营总监	服务经理	信息安全经理	业务连续性经理	法律顾问	审计
MEA04.01 确保鉴证提供商是独立的并且具有资质。			R	R	R	R						R	A
MEA04.02 制定基于风险的鉴证机制计划。	R	R	R	R		R						R	A
MEA04.03 确定鉴证机制的目标。	R	R	R	R		R						R	A
MEA04.04 定义鉴证机制的范围。	R	R	R	R		R						R	A
MEA04.05 定义鉴证机制的工作计划。	R		R	R		R						R	A
MEA04.06 执行鉴证机制，重点关注设计有效性。	R		R	R		R	R	R	R	R	R	R	A
MEA04.07 执行鉴证机制，重点关注运作有效性。	R		R	R		R	R	R	R	R	R	R	A
MEA04.08 报告和跟进鉴证机制。	R		R	R		R						R	A
MEA04.09 跟进建议和行动。	R	R	A	R		R		R				R	R

相关指南（标准、框架、合规性要求）	详细参考
本组件没有相关指南	

C. 组件：信息流和信息项（另请参阅第 3.6 节）				
管理实践	输入		输出	
MEA04.01 确保鉴证提供商是独立的并且具有资质。	自	描述	描述	至
			鉴证提供商评估的结果	内部
MEA04.02 制定基于风险的鉴证机制计划。	BAI01.05	计划的审计计划	鉴证计划	所有 APO；所有 BAI；所有 DSS；所有 MEA；EDM01.03
	DSS01.02	独立鉴证计划	评估标准	内部
			高层次评估	内部
MEA04.03 确定鉴证机制的目标。	MEA04.02	鉴证计划	鉴证目标和预期效益	内部
MEA04.04 定义鉴证机制的范围。	APO11.03	未能提供高品质的根本原因	鉴证审查实践	内部
	APO12.06	风险相关的根本原因	鉴证业务计划	内部
	DSS06.01	根本原因分析和建议		
	MEA03.04	不合规问题和根本原因的报告	鉴证审查范围	内部

C. 组件：信息流和信息项（另请参阅第 3.6 节）*（续）*				
管理实践	**输入**		**输出**	
MEA04.05 定义鉴证机制的工作计划。	**自**	**描述**	**描述**	**至**
	APO12.04	面向利益相关方的风险分析和风险概况报告	优化的范围	内部
			详细的鉴证工作方案	MEA04.06
MEA04.06 执行鉴证机制，重点关注设计有效性。	APO12.06	风险相关的根本原因	已记录的内部控制设计	MEA04.07
	DSS06.01	根本原因分析和建议		
	MEA04.05	详细的鉴证工作方案		
MEA04.07 执行鉴证机制，重点关注运作有效性。	DSS02.02	事故和服务请求日志	控制有效性测试	MEA04.08；MEA04.09
	DSS02.05	事故解决方案		
	DSS03.05	问题解决方案监控报告		
	DSS05.02	渗透试验的结果		
	DSS05.05	访问日志		
	DSS06.01	根本原因分析和建议		
	MEA04.06	已记录的内部控制设计		
MEA04.08 报告和跟进鉴证举措。	MEA03.03	已识别的合规性差距	鉴证审查报告	所有 APO；所有 BAI；所有 DSS；所有 MEA；EDM05.03
	MEA04.07	控制有效性测试	鉴证审查结果	所有 APO；所有 BAI；所有 DSS；所有 MEA；EDM05.03；MEA04.09
MEA04.09 跟进建议和行动。	MEA04.07	控制有效性测试	补救措施	所有 APO；所有 BAI；所有 DSS；所有 MEA
	MEA04.08	鉴证审查结果		
相关指南（标准、框架、合规性要求）		**详细参考**		
本组件没有相关指南				

D. 组件：人员、技能和胜任能力		
技能	**相关指南（标准、框架、合规性要求）**	**详细参考**
内部审计师学会® 描述的若干核心原则以支持（内部）审计职能的有效性和效率。这些原则包括独立的重要性、有效沟通技能和主动积极性等。	Core Principles for the Professional Practice of Internal Auditing，内部审计师学会	cfr.IIA — Standards & Guidance - Core Principles
风险管理	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework，2016 年	E. Manage—E.3. Risk Management

E. 组件：政策和程序			
相关政策	**政策描述**	**相关指南**	**详细参考**
鉴证指南	提供关于执行鉴证活动的指南。基于公认的鉴证方法制定高效和有效的 I&T 鉴证机制，包括规划、范围界定和执行鉴证审查。提供鉴证步骤来测试控制设计、测试控制的运作有效性结果，以及记录控制弱点及其影响。		
内部审计章程	提供执行审计审查的独立性并直接向最高管理层报告结果和建议。内部审计职能部门应该是一个独立的实体，向首席执行官或首席运营官报告工作。在 I&T 方面，章程应规定该职能部门负责审查一般控制和应用程序控制，以确定控制的设计是否符合管理方向、既定的标准和程序以及已知的法律要求，并且控制是否有效运行，为处理中的数据提供了可靠性和安全性（即机密性、完整性和可用性）。章程应规定内部审计职能部门负责审查新系统的设计、开发和实施或现有系统的重大修改。		

F. 组件：文化、道德和行为		
关键文化元素	**相关指南**	**详细参考**
营造乐于接受基于根本原因分析进行的内部审计和鉴证的结果及建议的文化。领导者必须确保内部审计和鉴证职能部门参与战略举措，并认识到审计和鉴证报告的必要性（和价值）。		
确保通过适当的道德规范形成合乎道德的内部审计文化。	道德规范，内部审计师学会	c\Standards & Guidnce - Co de of Ethics

G. 组件：服务、基础设施和应用程序
• 鉴证业务工具 • 事件日志审计工具 • 第三方鉴证供应服务

附录

5.1 附录 A：目标级联 — 对应关系表

附录 A 中的对应关系表显示了目标级联。第一张表展示了一致性目标与企业目标的对应关系；第二张表展示了治理和管理目标与一致性目标的对应关系。表中的 “P” 表示首要，“S” 表示次要。

5.1.1 对应关系表：企业目标 — 一致性目标

图 5.1 — 企业目标与一致性目标的对应关系

		EG01 有竞争力的产品和服务的组合	EG02 妥当管理的业务风险	EG03 遵守外部法律和法规	EG04 财务信息的质量	EG05 以客户为中心的服务文化	EG06 业务服务连续性和可用性	EG07 管理信息的质量	EG08 内部业务流程功能的优化	EG09 业务流程成本的优化	EG10 员工技能、动力和生产力	EG11 遵守内部政策	EG12 妥当管理的数字化转型计划	EG13 产品和业务创新
AG01	I&T 合规且支持业务部门遵守外部法律和法规		S	P								S		
AG02	妥善管理的 I&T 相关风险		P				S							
AG03	通过 I&T 促成的投资和服务组合所实现的效益	S				S			S	S			P	
AG04	技术相关财务信息的质量				P			P		P				
AG05	提供符合业务需求的 I&T 服务	P				S	S		S				S	
AG06	将业务需求转化为可运作的解决方案的敏捷性	P				S			S				S	S
AG07	信息、参与执行的基础设施和应用程序的安全，以及隐私的安全		P				P							
AG08	通过集成应用程序和技术来推行和支持业务流程	P				P			S		S		P	S
AG09	在预算内按时交付计划且满足要求和质量标准	P				S			S	S			P	S
AG10	I&T 管理信息的质量				P			P		S				
AG11	I&T 遵守内部政策		S	P								P		
AG12	既了解技术又熟知业务、能力出众且积极上进的员工					S					P			
AG13	业务创新的知识、专业技能和举措	P		S									S	P

5.1.2 对应关系表：一致性目标 — 治理和管理目标

图 5.2 — 治理和管理目标与一致性目标的对应关系

		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		I&T 合规且支持业务部门遵守外部法律和法规	妥善管理的 I&T 相关风险	通过 I&T 促成的投资和服务组合所实现的效益	技术相关财务信息的质量	提供符合业务需求的 I&T 服务	将业务需求转化为可运作的解决方案的敏捷性	信息、参与执行的基础设施和应用程序的安全，以及隐私的安全	通过集成应用程序和技术来推行和支持业务流程	在预算内按时交付计划且满足要求和质量标准	I&T 管理信息的质量	I&T 遵守内部政策	既了解技术又熟知业务、能力出众且积极上进的员工	业务创新的知识、专业技能和举措
EDM01	确保治理框架的设置和维护	P	S	P					S			S		
EDM02	确保实现效益			P		S	S		S					S
EDM03	确保风险优化	S	P					P				S		
EDM04	确保资源优化			S		S	S		S	P			S	
EDM05	确保利益相关方参与				S						P	S		
APO01	妥当管理的 I&T 管理框架	S	S	P		S		S	S	S	S	P		
APO02	妥当管理的战略			S		S	S		P				S	S
APO03	妥当管理的企业架构			S		S	P	S	P					
APO04	妥当管理的创新			S			P		S				S	P
APO05	妥当管理的组合			P		P	S		S	S				
APO06	妥当管理的预算和成本			S	P					P	S			
APO07	妥当管理的人力资源			S		S				S			P	P
APO08	妥当管理的关系			S		P	P		S	S			P	P
APO09	妥当管理的服务协议					P			S					
APO10	妥当管理的供应商					P	S			S				
APO11	妥当管理的质量			S	S	S				P	P			
APO12	妥当管理的风险		P					P						
APO13	妥当管理的安全	S	S					P						
APO14	妥当管理的数据	S	S		S			S			P			
BAI01	妥当管理的计划			P			S		S	P				
BAI02	妥当管理的需求定义			S		P	P		S	P			S	
BAI03	妥当管理的解决方案识别和构建			S		P	P		S	P				
BAI04	妥当管理的可用性和容量					P		S		S				
BAI05	妥当管理的组织变更			P		S	S		P	P			S	
BAI06	妥当管理的 IT 变更		S			S	P		S					
BAI07	妥当管理的 IT 变更接受和交接		S				P			S				
BAI08	妥当管理的知识			S			S		S	S			P	P
BAI09	妥当管理的资产				P						S			
BAI10	妥当管理的配置					S		P						
BAI11	妥当管理的项目			P		S	P			P				
DSS01	妥当管理的运营					P			S					
DSS02	妥当管理的服务请求和事故		S			P		S						
DSS03	妥当管理的问题		S			P		S						
DSS04	妥当管理的连续性		S			P		P						
DSS05	妥当管理的安全服务	S	P			S		P				S		
DSS06	妥当管理的业务流程控制		S			S		S	P			S		
MEA01	妥当管理的绩效和一致性监控	S		S		P				S	P	S		
MEA02	妥当管理的内部控制系统	S	S		S	S		S		S	S	P		
MEA03	妥当管理的外部要求合规性	P										S		
MEA04	妥当管理的鉴证	S	S		S	S		S			S	P		

5.2 附录 B：组织结构 — 概述和说明

在第 4 章的所有详细指南中，组织结构组件均源自**图 5.3** 中概述的角色和结构（另请参阅第 3.5 节的组织结构组件概述）。

在整个企业中，应用于每个角色或结构的术语可能有所不同。每个企业可按照以下说明，根据自身的业务背景、组织情况和运营环境来确定合适的角色和结构，并分配相应的职责和责任。

图 5.3 — COBIT 角色和组织结构

角色/结构	描述
董事会	企业的大多数高管和/或非执行董事组成的团队，负责企业资源的治理和总体控制
执行委员会	董事会任命的高管团队，旨在确保董事会参与重大决策并了解最新情况 （执行委员会负责管理 I&T 促成的投资组合、I&T 服务和 I&T 资产，确保价值得到实现并且风险受到管理。通常由董事会成员担任委员会主席。）
首席执行官	负责企业全面管理的最高级别官员
首席财务官	企业内负责所有财务管理方面事务的最高官员，包括财务风险和控制以及可靠、准确的账目
首席运营官	负责企业运营的最高官员
首席风险官	负责整个企业所有风险管理方面事务的最高官员 （可能会设立 I&T 风险官一职来监督 I&T 相关风险。）
首席信息官	企业内负责使 IT 和业务战略保持一致并负责规划、资源调配以及管理 I&T 服务和解决方案交付的最高官员
首席技术官	负责 I&T 技术方面的最高官员，包括管理和监控与 I&T 服务、解决方案和基础设施有关的决策 （此角色可能由 CIO 担任。）
首席数字官	负责实施企业或业务部门的数字化愿景的最高官员 （此角色可能由 CIO 或执行委员会的其他角色担任。）
I&T 治理委员会	利益相关方和专家组成的团队，负责指导 I&T 相关事务和决策，包括管理 I&T 支持的投资、实现价值和监控风险
架构委员会	利益相关方和专家组成的团队，负责指导企业架构相关事务和决策以及设定架构政策和标准
企业风险委员会	企业的高管团队组成的团队，负责支持企业风险管理 (ERM) 活动和决策所需的企业级合作和共识 （可能会建立 I&T 风险委员会来更详细地考虑 I&T 风险并向企业风险委员会提供建议。）
首席信息安全官	负责整个企业所有安全管理方面事务的最高官员
业务流程所有者	负责执行流程和/或实现流程目标、推动流程改进以及批准流程变更的个人
组合经理	负责指导组合管理，确保选择正确的计划和项目，管理和监控计划和项目以实现最佳价值，以及有效和高效地实现长期战略目标的个人
（计划/项目）指导委员会	利益相关方和专家组成的团队，负责指导计划和项目，包括管理和监控计划、分配资源、实现效益和价值以及管理计划和项目风险
计划经理	负责指导特定计划的个人，包括阐明和跟进计划的目的和目标，以及管理风险及其对业务的影响

图 5.3 — COBIT 5 角色和组织结构（续）	
角色/结构	**描述**
项目经理	负责指导特定项目的个人，包括协调和分配整个项目团队的时间、预算、资源和任务
项目管理办公室	负责支持计划和项目经理以及收集、评估和报告有关其计划和组成项目执行情况的职能部门
数据管理职能部门	负责在整个数据生命周期中支持企业数据资产以及管理数据战略、基础设施和贮存库的职能部门
人力资源总监	负责企业内人力资源方面的规划和政策的最高官员
关系经理	负责监督和管理业务职能部门与 I&T 职能部门之间的内部接口和沟通的高级管理人员
架构总监	负责企业架构流程的高级管理人员
开发总监	负责 I&T 相关解决方案开发流程的高级管理人员
IT 运营总监	负责 IT 运营环境和基础设施的高级管理人员
IT 行政总监	负责 I&T 相关记录并负责支持 I&T 相关行政事务的高级管理人员
服务经理	面向特定客户（用户）或客户（用户）群体管理新的及现有产品与服务的开发、实施、评估和持续维护的个人
信息安全经理	管理、设计、监督和/或评估企业的信息安全的个人
业务连续性经理	管理、设计、监督和/或评估企业的业务连续性能力，以确保企业的关键职能部门在破坏性事件后继续运作的个人
隐私官	负责监控隐私法律的风险和业务影响并指导和协调政策及活动实施，以确保遵守隐私指令的个人 （有些企业称这一职位为“数据保护官”。）
法律顾问	负责指导法律和法规事务的职能部门
合规	负责提供所有关于外部合规性指导的职能部门
审计	负责提供内部审计的职能部门

5.3 附录 C：详细的参考文献列表

以下标准和指南提供了 COBIT® 2019 的 40 项核心治理和管理目标的详细参考。

- CIS® 互联网安全中心®，*The CIS Critical Security Controls for Effective Cyber Defense*，第 6.1 版，2016 年 8 月
- CMMI® Cybermaturity Platform，2018 年
- CMMI® 数据管理成熟度 (DMM)℠ 模型，2014 年
- 发起组织委员会 (COSO) 企业风险管理 (ERM) 框架，2017 年 6 月
- 欧洲标准化委员会 (CEN)，*e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework*, EN 16234-1:2016

- HITRUST® 通用安全框架，第 9 版，2017 年 9 月
- 信息安全论坛 (ISF)，*The Standard of Good Practice for Information Security 2016*
- 国际标准化组织/国际电工技术委员会 (ISO/IEC) 标准
  - ISO/IEC 20000-1:2011(E)
  - ISO/IEC 27001:2013/Cor.2:2015(E)
  - ISO/IEC 27002:2013/Cor.2:2015(E)
  - ISO/IEC 27004:2016(E)
  - ISO/IEC 27005:2011(E)
  - ISO/IEC 38500:2015(E)
  - ISO/IEC 38502:2017(E)
- 信息技术基础设施库 (ITIL®)，第 3 版，2011 年
- 内部审计师学会® (IIA®)，“Core Principles for the Professional Practice of Internal Auditing”
- *King IV Report on Corporate Governance*™，2016 年
- 美国国家标准与技术研究所 (NIST) 标准
  - *Framework for Improving Critical Infrastructure Cybersecurity*，第 1.1 版，2018 年 4 月
  - 特别出版物 800-37，修订版 2（草稿），2018 年 5 月
  - 特别出版物 800-53，修订版 5（草稿），2017 年 8 月
- *A Guide to the Project Management Body of Knowledge: PMBOK® Guide*，第 6 版，2017 年
- PROSCI® 3-Phase Change Management Process
- Scaled Agile Framework for Lean Enterprises (SAFe®)
- Skills Framework for the Information Age (SFIA®)，第 6 版，2015 年
- The Open Group IT4IT® Reference Architecture，第 2.0 版
- The Open Group Standard TOGAF®，第 9.2 版，2018 年