Modern Management 现代管理, 2021, 11(2), 96-103
Published Online February 2021 in Hans. http://www.hanspub.org/journal/mm
https://doi.org/10.12677/mm.2021.112012

Hans汉斯

公司治理层面的信息系统内部控制探析

——基于 COBIT2019 框架

郭　群[1]，包经纬[2]

[1]中山大学管理学院现代会计研究中心，广东　广州
[2]中山大学南方学院，广东　广州
Email: mnsgq@mail.sysu.edu.cn

收稿日期：2021年1月18日；录用日期：2021年2月8日；发布日期：2021年2月22日

摘　要

随着信息技术的快速发展，信息系统在企业发展中的地位越来越重要，信息系统已经不再是企业的一个技术部门，而成为企业经营活动不可或缺的重要组成部分。COBIT2019框架是国际公认的信息系统治理框架，为企业信息系统治理提供参考。文本从公司治理层面探讨企业信息系统的治理要求，从企业风险优化和资源优化的视角，将信息系统与企业治理方法相结合，并与企业的战略目标保持一致，实现企业价值创造。

关键词

公司治理，信息系统内部控制，COBIT2019框架

Analysis on the Internal Control of Information System of Corporate Governance

—Based on the COBIT2019 Framework

Qun Guo[1], Jingwei Bao[2]

[1]Sun Yat-sen University Research Center of Modern Accounting, Guangzhou Guangdong
[2]Nanfan College of Sun Yat-sen University, Guangzhou Guangdong
Email: mnsgq@mail.sysu.edu.cn

Received: Jan. 18th, 2021; accepted: Feb. 8th, 2021; published: Feb. 22nd, 2021

文章引用: 郭群, 包经纬. 公司治理层面的信息系统内部控制探析[J]. 现代管理, 2021, 11(2): 96-103.
DOI: 10.12677/mm.2021.112012

Abstract

With the rapid development of information technology, the status of information system in the development of enterprises is more and more important. Information system is no longer a technical department of the enterprise and has become an indispensable part of business activities of enterprises. The COBIT2019 framework is an internationally recognized information system governance framework. It discusses internal control of information systems from the perspective of corporate governance, combines information systems with corporate governance methods from the perspective of risk optimization and resource optimization, and keeps consistent with the strategic objectives of the enterprise to achieve value creation.

Keywords

Corporate Governance, Internal Control of Information System, COBIT2019 Framework

1. 引言

随着当前信息技术的迅猛发展，企业的工作逐渐转向无纸化，数据存储和处理方式发生了巨大的改变，企业的发展也更依赖信息系统，信息系统在企业发展中的地位越来越重要，信息系统内部控制的重要性也越发凸显。我国企业对于信息系统内部控制的重视程度逐渐提高，对信息系统内部控制进行研究，有利于防范风险、提升效益并实现资源的优化。应对企业中与信息系统相关的业务风险，包括可能对业务产生影响的信息系统相关事件，将信息系统相关风险的管理整合到企业内部控制中，以确保企业对信息系统风险的防范。但目前我国对于信息系统内部控制的实施尚缺少明确的指导标准，相当一部分企业仍旧将信息系统作为一种技术工具，未能从战略视角重视信息系统的建设，导致信息系统无法持续支持企业战略。本文借鉴国际公认的信息系统内部控制标准 COBIT 框架，从公司治理层面探讨企业信息系统的治理要求，从风险优化和资源优化的视角，将信息系统与企业治理方法相结合，并与企业的战略目标保持一致。

2. 信息系统内部控制概念与演进

2.1. 信息技术与信息系统

信息技术(Information Technology，缩写 IT)，主要是指用于管理和处理信息的各种技术，通过应用计算机科学和通信技术来设计、开发、安装和实施信息系统及应用软件。信息系统(Information System，缩写 IS)，是人机一体化系统，由硬件、软件、信息资源、信息用户和相关的规章制度而组成的，以处理信息流为目的[1]。信息系统与信息技术存在以下区别：首先，在组成要件方面，信息技术主要侧重于硬件设备，信息系统着重于对各种信息技术进行组织以及管理，使其组成整体，以达到系统的目的。其次，在功能方面，信息技术侧重于信息的采集、识别和传递，而信息系统则侧重于信息的处理及管理。第三，在使用方面，信息技术更靠近信息源，信息系统更靠近信息使用者。信息技术是信息系统的基础，是构成信息系统的要素，信息系统正是将各种信息技术有机地组合在一起，才能实现其系统的功能和目的。

如果没有信息系统的支持，信息技术也不可能有效地发挥其功能。信息系统对信息技术读取的信息进行存储、转换、识别、传递并输出给用户，如若缺少信息系统的输出，信息技术读取的信息也就不能发挥应有的作用。

我国《企业内部控制应用指引第 18 号——信息系统》中明确指出[2]，信息系统是企业利用计算机和通信技术进行内部控制的信息化管理平台，在传统内部控制基础上进行集成、转化和提升。其组成要素包括硬件、软件、人员、信息流以及运行规程，信息系统内部控制的目标主要包括企业内部控制目标、信息系统目标以及信息目标三个层面，企业内部控制目标主要是为了促进企业实施内部控制的有效性，提高企业现代化管理水平，减少人为操纵因素；信息系统目标主要是促进信息系统更为安全、可靠和合理；信息层面的目标是通过加强信息系统内部控制以确保信息的保密、完整和可用，为提高信息与沟通机制的有效性提供支持与保障。COSO 框架(2013 版)指出，信息系统和相关技术的发展，已经极大的改变了企业信息系统和内部控制流程的实施和管理。如今，信息系统已经成为内部控制流程设立、嵌入和运营自动化的载体[3]。信息系统控制分为一般控制和应用控制，一般控制涵盖了信息系统运营的各个方面，例如系统运行、编程和录入数据、程序开发和程序变换、网络控制等；应用控制是涉及具体应用过程的应用程序控制，如应付账款应用程序。应用控制功能的发挥依赖于一般控制的支持，一般控制因为应用控制的存在而对企业具有实际意义，它们之间存在着相互依赖和相互支持的关系，只有两者共同发挥作用才能使信息系统在加强企业管理和实现控制方面发挥其独特的优势[4]。COSO 框架在“信息与沟通”要素部分指出[5]，信息系统是企业经营不可缺少的一个组成部分，信息系统不仅通过提供决策所需要的信息来影响控制，而且还是支持企业战略、实现战略目标的重要手段。信息系统的战略性应用，要求突破单一的财务信息系统而扩展到财务与业务集成的企业管理信息系统，这样有利于控制业务流程并实时跟踪和记录交易。

2.2. 信息系统内部控制演进

ISACA (信息系统审计与控制协会)，是全球公认的研究信息与网络安全、治理、鉴证的组织，该协会于 1996 年开始发布 COBIT (Control Objectives for Information and related Technology，以下简称 COBIT)的第一版，它最初主要是作为一种审计工具，内容上包括控制目标及评价标准。COBIT1.0 汲取其他有关 IT 方面的国际准则及研究成果，将企业业务流程中的控制需求置于 IT 流程之内，得到广泛的认可。随着信息技术的发展，IT 对企业的重要性不断增强，在近十多年 COBIT 也随着不断完善(见图 1)。1998 年，COBIT2.0 正式发布，对信息系统控制框架与控制目标进行改进和完善，增加了实施工具集。2000 年，ITGI (Information Technology Governance Institute)，即信息技术治理协会[1]，继续对 COBIT 框架进行完善与升级，并积极促进其应用与推广，发布 COBIT3.0，增加管理指南，主要包括目标成熟度模型、关键目标以及关键绩效指标等。ITGI 于 2005 年推出 COBIT4.0，引入了 IT 治理的概念，将 IT 治理与 IT 管理有机结合，更好地指导和帮助治理层与管理层对 IT 控制和运用。2007 年，ITGI 继续推出 COBIT4.1，在内容上调整了 IT 治理中对于 IT 控制的监督与评价；对关键目标和关键绩效指标进行更为详细的阐述和说明；重新定义相关概念；并对控制措施进行改进与完善等[6]。2013 年，ISACA 发布 COBIT5.0。与之前的版本相比，COBIT5.0 的改变主要表现在以下几个方面：首先，广泛借鉴企业信息安全模型、信息保障技术框架等与之相关的国际准则[2]的优点；其次，明确区分治理与管理流程，定位为信息系统治理与管理框架，扩大了其实际运用范围；第三，融合了理论基础与业务视角，明确了各利益相关方的需求，将业务

[1]1998 年，ISACA 与 ISACF 合并为 ITGI (Information Technology Governance Institute，简称 ITGI)。
[2]相关国际组织与准则包括：ITIL (信息技术基础架构库)、TOGAF (开放组体系结构框架)，以及国际标准化组织与国际电工委员会联合制定的 ISO15504、IT 治理国际标准 ISO38500 等。

需求与技术问题结合起来，以探讨信息系统治理与管理的价值；第四，为了促进对信息系统进行更恰当地控制与评价，更新了成熟度模型的级别以及流程的具体描述[6]。

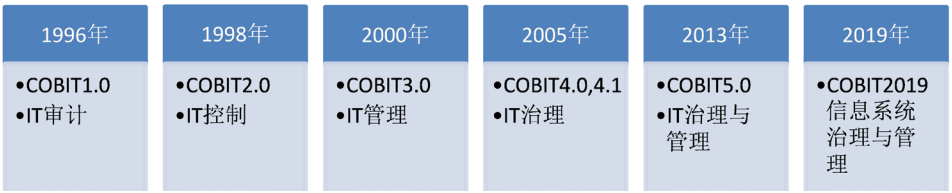


Figure 1. Evolution course of COBIT
图 1. COBIT 的演进

COBIT 从最初的审计工具发展成为更为广泛而全面的信息系统治理与管理框架，该框架体系已在世界上获得高度认可与广泛运用，成为国际上公认的信息系统治理和管理的框架，指导企业更有效地利用信息资源，推动企业信息系统内部控制的完善和改进。

3. COBIT2019 及特点分析

3.1. COBIT2019 框架

信息技术在企业发展中的地位越来越重要，林斌等(2016)认为，随着“互联网+”国家战略的逐步推行，IT 成为现代企业关键战略要素之一，未来企业经营必将处于高度信息化环境之下[7]。企业的发展极大程度依赖于信息系统，信息系统内部控制的风险管理也越发凸显。从企业治理层面，过去企业可能忽略了与信息系统相关的决策，但如今企业必须考虑信息系统在企业风险管理和价值创造中起到的核心作用，COBIT2019 框架应运而生。COBIT2019 框架包括四个部分：简介与方法、治理与管理目标、设计指南及实施指南[8]。COBIT2019 框架以风险优化为基本目标，将信息系统相关风险，以及信息系统可能对业务产生的风险，整合到企业风险管理之中，以确保企业对信息系统及内部控制的关注。同时提出通过资源优化确保企业有适当的能力执行战略规划，数据和信息是企业重要的资源，根据业务需要引入新技术、更新过时的系统，高效综合的基础设施，确保企业战略规划的执行，利用数据和信息为企业创造价值。例如，某大型国际化企业，通过增加数字资产投资，持续提高信息系统创新能力与企业战略目标的一致性，加深经营活动与信息系统的关联，成功实现数字资产创造价值的转型。相反，如果企业信息系统治理未能与企业战略及业务流程一致，则难以实现预期的价值创造。COBIT2019 框架立足于审计领域，已发展为一种更广泛、更全面的信息系统治理与管理框架。

3.2. COBIT2019 框架特点分析

3.2.1. COBIT2019 治理原则

COBIT2019 治理原则包括：为利益相关方创造价值、整体的方法、动态的治理系统、治理有别于管理、根据企业需求量身定制以及端对端的治理系统等六项[9]。与 COBIT5.0 相比，COBIT 2019 治理原则，把满足利益相关方的价值需求放在第一位，即企业价值创造应反映整个供应链的效益、风险与资源之间的平衡，需要可行的战略和治理系统的基础上，应通过使用信息系统为企业创造价值，并突出企业信息系统治理应该是动态的，每当变更一个或多个设计因素，如战略或技术变更时，必须考虑这些变化对信息系统的影响，根据企业需求量身定制。

3.2.2. COBIT2019 治理框架

COBIT2019 新增治理框架，即基于概念模型，强调开放性、灵活性、规范性和相关性，并符合主要

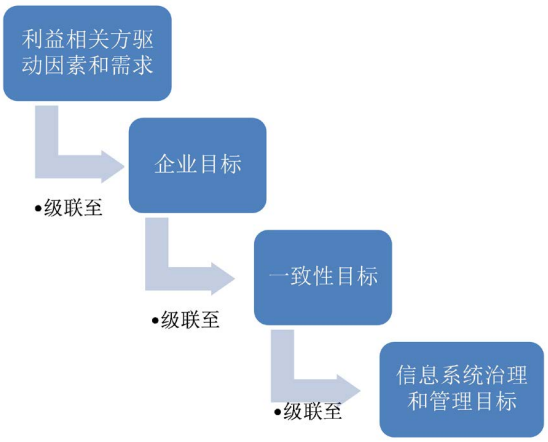
标准。治理框架应当基于概念模型，再对治理框架的关键组件以及组件之间的关系进行确定，在与概念模型一致性的前提下实现自动化。同时，治理框架允许在保持完整的框架结构基础上增加新的内容，使得治理框架在遵守相关的法律法规、其他框架标准的基础上具有开放性和灵活性。COBIT2019 治理框架中阐述了信息系统治理与管理目标、治理体系组件、焦点领域、目标级联等。

控制目标分为治理和管理目标，分别与治理流程和管理流程有关。COBIT 中的治理目标包括评估、指导和监督，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、计划和组织阶段；构建、购置和实施阶段；交付、服务和支持阶段；监控、评价和评估阶段，共 40 个治理和管理目标。为满足治理和管理目标，每个企业都需要建立和维护由多个组件构成的内部控制体系，组件是单独或共同促进企业的信息系统良好运营的因素。信息系统内部控制组件包括设计流程、组织结构、政策和程序、信息、文化、道德行为、技能和能力以及服务、基础设施和应用程序等。

3.2.3. COBIT2019 设计因素与焦点领域

COBIT2019 遵循灵活性和开放性原则，新增设计因素与焦点领域的内容，为企业基于自身条件及需求对治理系统进行量身定制的设计提供基础。影响信息系统内部控制设计的因素包括企业战略、企业目标、风险概况、信息系统相关问题、威胁环境、合规性要求、信息系统定位、采购模式、信息系统实施方法、以及企业规模等。每个企业在信息系统使用过程中都有不同的期望，需要针对不同企业的特点，结合 COBIT 的设计因素，以确定不同企业信息系统内部控制的要求。焦点领域描述某个特定的治理主体或领域，可以通过一系列治理和管理目标及其组件来实现。COBIT 对于焦点领域的内容和数量并没有限制，企业可根据需要进行设置，通常设为焦点领域的如：网络安全、数字化转型、云计算等。

企业对于利益相关方需要的考虑应转换为可执行的战略，目标级联(见图 2)是信息系统内部控制设计的关键因素之一，它是基于企业目标的优先级来确定管理目标的优先级，一致性强调信息系统目标与企业业务活动目标保持一致。



资料来源：根据 ISACA 网站整理。

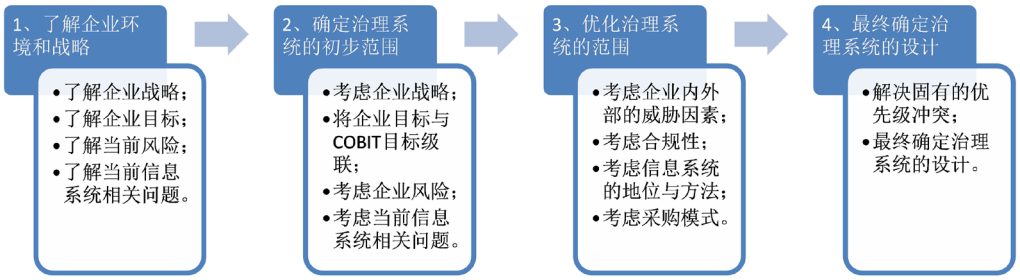
Figure 2. COBIT target cascading
图 2. COBIT 目标级联

焦点领域和设计因素会影响管理目标优先级和目标能力级别，在 COBIT 框架中包含的治理与管理控制目标本质上没有先后顺序，但设计因素可以影响这些目标的管理，突出一些目标的重要性，治理和管理目标的重要性越高，为其设定的目标能力级别越高。设计因素可以要求特定的组件变化，影响组件的

重要性，如中小企业不需要 COBIT 框架中的全套角色和组织结构，可以使用简化版本作为代替。对特定焦点领域的指导，特定的设计因素，如存在威胁的环境、特定风险等会推动 COBIT 模型的内容随着具体环境变化。

3.2.4. COBIT2019 治理流程设计

在 COBIT2019 实施指南强调，企业治理层应从企业的战略角度考虑信息系统内部控制。由于信息系统已经渗透到企业的每个角落，已成为企业的重要组成部分，如果不能把信息系统与业务活动相互结合，那么信息系统将无法发挥应有的作用。因此，企业应将信息系统内部控制作为公司治理的重要组成，嵌入持续经营的业务活动之中，履行全面覆盖端到端的业务和信息处理的职责。信息系统治理流程见图 3。



资料来源：根据 ISACA 网站整理。

Figure 3. Information system governance process
图 3. 信息系统治理流程

3.2.5. COBIT2019 绩效管理

绩效管理是企业治理与管理系统中不可或缺的重要内容，COBIT2019 新增绩效管理的相关内容。COBIT 绩效管理强调企业治理与管理系统所涉及的组件的运作状况及存在的问题。COBIT 绩效管理采用对系统流程能力分级的方式，将每个治理与管理目标的流程能力划分 0 到 5 的不同级别，构建流程能力级别模型，对流程的实施和执行情况进行评价。根据流程能力级别模型，对焦点领域的单个流程能力采用成熟度级别评级，同样划分 0 到 5 的成熟度级别，即评价焦点领域的全部流程是否达到一定能力级别，如果达到，那么焦点领域也就达到对应的成熟度级别(见表 1)。另外，COBIT2019 也对其他治理系统组件的绩效进行说明，例如组织中对应的责任人与执行人的相关责任与职责进行评价。

Table 1. Process capability level model and focus hierarchical performance evaluation
表 1. 流程能力级别模型与焦点领域分级绩效评价

级别	流程能力	焦点领域成熟度
0	缺乏基本能力；以不完整的方法达成治理和管理目标；可能无法达成流程的目的。	不完整，可能无法完成工作，以实现焦点领域的治理和管理目标。
1	具有初始、直观的特征；条理不够清晰；大体达成其目的。	初始，工作已完成，但尚未实现焦点领域的所有目标和意图。
2	视为“已执行”，基本达成其目的。	已管理，执行规划和绩效管理，但不是以标准化方式进行。
3	流程定义明确，以更有条理的方式达成其目的。	明确定义，以企业范围的标准为整个企业提供指导。
4	流程定义明确，达成其目的，并且流程绩效得到定量方式的评价。	量化，企业以数据为导向，采用量化的绩效管理。
5	流程定义明确，达成其目的，流程绩效得到定量方式的评价以实现改进，并寻求持续改进。	持续优化，企业专注于持续的改进。

资料来源：根据 ISACA 网站整理。

4. 结论与启示

通过上文对 COBIT 框架的发展过程以及 COBIT2019 详细的分析，并结合我国企业实施与执行信息系统内部控制的现状，我们认为，未来的企业必将置于高度信息化的环境之中，信息系统设计与完善已成为影响企业发展的重要战略因素，企业必须从治理层面，从战略的视角推动信息化与业务流程的结合，以 COBIT2019 框架为指导，持续强化信息系统内部控制防范系统风险。

4.1. 完善企业治理结构，建立信息系统治理委员会

当前，企业信息系统已成为企业的核心竞争力之一，企业需要提高对信息系统及其内部控制的重视程度[10]。在企业层面，要从战略角度进行信息系统治理，而不能将信息系统作为一个执行业务活动的具体部门管理，如在公司董事会层面建立起信息系统治理委员会，完善公司治理结构，规范企业信息系统治理流程和治理机制，进而有效推进信息系统内部控制，有效防范系统风险，实现企业战略目标。Turel 和 Bart (2014)发现，董事会层面的信息系统治理有助于提升企业的业绩[11]。将信息系统治理融入到公司治理之中，有助于推进信息系统治理作用的发挥。在董事会中设置信息系统治理委员会，涵盖信息技术部门、业务部门、财务部门以及内部审计部门，可以提高信息系统对企业价值创造的贡献，避免过高的成本导致的资源浪费，及时发现系统建设及运行中存在的问题。

4.2. 区分治理与管理，体现信息系统内部控制的战略地位

COBIT 早期的版本并没有区分治理层与管理层的责任，只是以 IT 技术服务企业的业务流程，是一种狭义的管理观。从 COBIT5 开始，将治理与管理相区分，为企业制定了良好的治理与管理基调。COBIT2019 治理与管理目标结构中进一步规范治理与管理，将信息系统治理责任上升到董事会的职责范畴内，提出组织中增加首席信息安全官、首席数字官等角色。董事会制定的治理目标定位在评估、指导和监督管理层实现信息系统的管理责任，管理层责任则在于信息系统的调整、规划与组织、内部构建与实施及交付、服务与支持等。区分治理与管理，清晰划分相关责任，将信息系统内部控制提升到战略的高度，与企业的战略目标保持一致，确保信息系统相关流程得到有效和透明的监督，满足企业治理的要求。

4.3. 满足利益相关者需求，以价值创造为企业终极目标

随着信息技术的发展，企业与利益相关者的关系越来越紧密，企业信息系统的建设与运行不仅与企业内部业务相关，还应该考虑供应商、客户等利益相关者的需求。COBIT2019 强调满足利益相关者的需求，以价值创造为信息系统治理的目标。企业与利益相关者形成一条价值链，不在是信息孤岛，利益相关者的行为、决策同样也会对企业产生影响。因此，企业需要考虑利益相关者需求，从战略高度建立企业目标，将董事会、管理层及信息系统整合起来，从企业整体的视角，与供应商与客户建立密切合作关系，可以通过对信息系统及相关服务的供应链上下游进行整合，发掘信息系统的潜在价值，促进企业战略目标的实现。

4.4. 强调文化、道德和行为建设，营造良好信息系统运营环境

COSO 框架(2013)原则 1 首先强调“对诚信和道德价值的承诺”；COBIT5 首次将文化、道德和行为作为信息系统内部控制重要因素之一，强调其在实现信息系统治理目标中的重要作用。COBIT2019 绩效管理中指出，对于文化、道德和行为，应作为信息系统的组件，可针对良好的信息系统治理与管理定义一组可取或不可取的行为，并为每个行为分配不同的级别，据此做出评估。可见，文化、道德和行为的软控制，已成为信息系统内部控制的重要手段之一。强调文化、道德和行为建设，有助于营造良好的内

控环境，更好地发挥员工个体能动性，有助于治理目标的实现。

参考文献

[1] 章铁生. 信息技术条件下的内部控制规范: 国际实践与启示[J]. 会计研究, 2007(7): 29-35.

[2] 企业内部控制编审委员会, 编著. 企业内部控制: 主要风险点、关键控制点与案例解析[M]. 上海: 立信会计出版社, 2020: 377-380.

[3] (美)罗伯特. R. 穆勒, 著. 2013 版 COSO 内部控制指南[M]. 秦荣生, 张庆龙, 译. 北京: 电子工业出版社, 2015: 35-38.

[4] 刘永泽, 池国华, 主编. 企业内部控制[M]. 北京: 清华大学出版社, 2014: 160-165.

[5] 方红星, 主编. 内部控制[M]. 第 4 版. 大连: 东北财经大学出版社, 2019: 26-31.

[6] 王会金, 刘国城. COBIT 模型及其在中观经济主体信息系统审计中的运用[J]. 审计研究, 2009(1): 64-68.

[7] 林斌, 曹键, 舒伟. 信息技术内部控制研究——基于 COBIT2015 的分析[J]. 江西财经大学学报, 2016(1): 36-43.

[8] CBOIT2019 Design Guide: Designing an Information and Technology Governance Solution. ISBN 978-1-60420-765-1.

[9] COBIT 2019 Framework: Introduction and Methodology. ISBN 978-1-60420-763-7.

[10] 骆良彬, 张白. 企业信息化过程中内部控制问题研究[J]. 会计研究, 2008(5): 69-75.

[11] Turel, O. and Bart, C. (2014) Board-Level IT Governance and Organizational Performance. *European Journal of Information Systems*, **23**, 223-239. https://doi.org/10.1057/ejis.2012.61