ISO/IEC 38500:2008

第一版

2008-06-01

Corporate governance of information technology

组织的信息技术治理

目录

前言

ISO（国际标准化组织）和IEC （国际电工委员会）构成世界范围内的标准化专门体系。国家组织作为ISO或IEC的成员，通过由处理特定技术领域的相应组织所建立的技术委员会参与开发国际标准。ISO和IEC的技术委员会在共同关心的领域合作。其他的国际性组织，官方或非官方的，也与ISO和IEC联系，参与部分工作。在信息技术领域，ISO/IEC 建立了联合技术委员会， IEO/IEC JTC 1。

国际标准依据ISO/IEC 指南第2部分起草。

联合技术委员会的主要任务是准备国际标准。 联合技术委员会接受的国际标准草案将提交过国家组织进行投票。成为国际标准公开发布，则需要至少75%的国家组织投赞成票。

应注意本标准的某些内容可能涉及专利。ISO和IEC不负责识别任何专利。

ISO/IEC 38500S 由澳大利亚标准（AS8015:2005）起草，并ISO/IEC JCT1信息技术联合技术委员会按快速跟踪程序所采纳，并得到了ISO和IEC 的国家组织批准。

ISO/IEC 38500 是基本性的、原则性的建议标准。另外，为了向管理团队提供组织广泛的指导，鼓励组织使用适当的标准去支撑IT治理。

在发布本标准时，JTC1正在继续努力开发更多信息技术治理文件。这些文件很可能在将来以ISO/IEC 技术报告或标准的形式发布，预期涉及的主题包括：

– 与IT投资相关的项目治理

– 持续业务运营所使用的IT的治理

介绍

本标准旨在为领导者在组织内评估、领导和监控信息技术（IT）的使用，提供一个原则框架。

大部分组织使用IT 作为一个基本的业务工具，很少的业务功能在没有IT时可以有效运作。对于很多组织，IT也是将来业务规划的重要因素。

IT支出占组织财务和人力资源支出的重要部分。但其投资的收益常常没有得到充分认识，而且可能会给组织带来重大的负面影响。

这些消极结果的主要原因是，过于强调IT活动的技术、财务和日程安排方面，而没有关注整个业务环境中的IT使用。

本标准针提供IT的有效治理的框架，以帮助组织高层人员理解和实现其组织在利用IT方面的法律、法规和道德要求。

此框架由定义、原则和模型组成。

本标准与作为企业治理财务领域委员会1992年报告（Cadbury 报告）发表的组织治理相一致。Cadbury 报告也为1999 年的OECD企业治理原则（2004进行的修订）提供了企业治理的基本定义。本标准鼓励标准的使用者去理解Cadbury 报告和OECD 企业治理原则。

治理不同于管理，为避免混淆，在本标准中对这两个概念进行了清晰定义。

当本标准服务于治理团队，反过来也可能领导组织管理层采取的某些行动。在一些组织（通常是小型组织），允许治理团队成员承担管理的关键角色。在这个意义上，它可以确保本标准适用于所有组织，无论大型组织，还是小型组织，而不论组织的目的、规划和股东结构；

本标准旨在为参与设计和实施支持治理的管理体系方针、流程和结构的人员提供信息和指南。

组织的信息技术治理

1. 范围、应用和目标

1.1. 范围

本国际标准为组织的责任人（包括所有者、董事会成员、责任人、合作伙伴、高级执行层，或其他类似人员）提供组织内有效、高效和合理运用信息技术（IT）的指导性原则。

本标准用于组织内部信息和通讯服务的管理流程（和决策）的治理。这些过程可能受组织内的IT专家、外部服务提供商或组织内业务部门控制。

本标准也为那些给向组织的责任人进行建议、告知或协助的人员提供指南。包括：

- 高层管理者
- 监视组织资源利用的小组成员；
- 外部的业务或技术专家，如法律或财务的人员；专家；零售业协会，或专业团体；
- 软件、硬件、通讯或其他IT产品的供应商；
- 内部或外部服务提供方（包括咨询人员）；
- IT审计人员。

1.2. 应用

本标准适用于所有组织，包括公众和私有公司、政府组织和非赢利组织。本标准也适用于从小型到大型不同规模的组织，而不论其对IT利用的程度。

1.3. Objectives 目标

本标准目的是通过以下方式，促进所有组织有效、高效和合理的利用IT：

- 遵循本标准，可能使得相关利益方（包括消费者、股东和雇员）对组织的组织IT治理的具有信心；

- 为组织内治理IT使用的责任人提供信息和指导；
- 为组织的IT治理提供基本的客观评估。

1.4. 使用本标准带来的好处

1.4.1. 总则

本标准建立有效、高效和可接受的利用IT的原则。确保组织依据这些原则，将有助于责任人平衡风险和鼓励从IT使用中获得机会。

本标准建立了IT治理的模型。通过对IT治理原则模型的合理应用，可以降低责任人未能履行其职责的风险。

本标准还提供了有关IT治理的术语。

1.4.2. 组织的符合性

合适的IT治理能够帮助责任人确保组织在可接受的IT利用方面，符合职责和义务（法律法规、合同）要求。

不恰当的IT系统可能使责任人面临不符合法律要求的风险。如在某些判决中，不适当的财务系统导致没有交税，责任者个人可能需承担责任。

涉及IT的过程具有特定的风险，必需适当处理。如，责任人可能要为以下的违背行为承担责任：

- 安全标准；
- 隐私保护法律；
- 垃圾邮件法规；
- 贸易惯例法规；
- 知识产权，包括软件许可协议；
- 记录保存的要求；
- 环境相关的法律法规；

- 健康和安全的法规；
- 残疾人便利法规；
- 社会责任标准。

领导者利用本标准的指南，可最大程度的满足其责任的要求。

1.4.3. 组织的绩效

适当的IT治理通过以下活动，帮助领导者确保IT的利用将为提高组织绩效带来积极的影响：

- 合理的实施和运行IT资产；
- 明确达成组织目标的IT的使用者和提供方的职责和责任；
- 业务连续性和稳定性；
- IT与业务要求的一致性；
- 有效分配资源；
- 服务、市场和业务的创新；
- 维持与利益相关方关系的良好实践；
- 降低组织成本；以及
- 实际认识到从每一IT投资获得的经过认可的收益。

1.5. 参考文献

本标准引用了以下文献：

- 组织财务治理报告, Sir Adrian Cadbury, 伦敦, 1992 ISBN 0 85258 913 1
- OECD 组织治理原则, OECD, 1999 and 2004
- ISO 指南73 2002 - 风险管理 - 术语 – 标准使用指南。

1.6. 定义

以下定义适用于本标准。

希望组织在其环境和架构中采用本标准的术语。

1.6.1. 可接受的

满足利益相关方的合理或应得的期望。

1.6.2. 组织治理

组织领导和控制体系。（引自Cadbury 1992 and OECD 1999）

1.6.3. 组织的 IT 治理

领导和控制当前和将来IT利用的体系。

IT治理涉及评估和领导支持组织的IT的使用，并监视IT的使用，以实现计划。它包括组织内IT使用的策略和方针。

1.6.4. 能力

具有履行一项任务或角色所需的知识、正式或非正式的技能、培训、经验和行为的综合特性。

1.6.5. 领导者

组织最高层治理团体的成员。包括所有者、董事会成员、合伙人、高层执行人或其他类似人员，以及法定的人员。

1.6.6. 人员行为

理解人员之间，以及与体系其他元素的之间的相互作用，以确保得到良好的感知和体系的绩效。人员行为包括作为个人或团队的文化、需求及志向。

注：对于IT，存在多种人员团体和小组，都具有其自身的需求、志向及行为。如，使用信息系统的人员可能展示访问便利、人体工程学以及可用性和和性能相关的要求。工作角色因IT应用而改变的

人员可能展示的需求，是与沟通、培训和信心恢复相关的。建立和运行IT的人员可能展示的需求是，关于工作条件和开发技能的。

1.6.7. 信息技术（IT）

获得、处理、保存和传播信息所需的资源。该术语可能包括“通讯技术（CT）” 和组合术语“信息与通讯技术（ICT）”。

1.6.8. I 投资

分配人员、资金和其他资源以达成既定目标和获得其他利益。

1.6.9. 管理

为达到组织治理团队所设置的策略性目标所需的控制和过程体系。管理受制于组织治理所设定的方针指南和监视。

1.6.10. 组织

具有自身职能和管理的任何公司、企业、政府、非赢利或其他合法组织，包括协会、俱乐部、合作企业、政府组织、公众公司、私有公司及专营商等。

1.6.11. 方针

有关首要方向和行为的、明确和可衡量的描述，以约束组织内的决策。

1.6.12. 建议

收益、成本、风险、机会和其他适用于做出决策的因素的文档，包括业务案例。

1.6.13. 资源

人员、程序、软件、信息、设备、耗材、基础设施、资金和运作基金，以及时间。

1.6.14. 风险

事件可能性和后果的组合 (ISO/IEC Guide 73).

注：后果是对组织的影响。后果可能是负面的，作为通常用法，对应的是“机会”。

1.6.15. 风险管理

领导和控制组织风险的协调活动（ISO/IEC Guide 73）。

1.6.16. 利益相关方

可能影响某一决策或活动，可能受到某一决策活动影响或自身感知受到影响的任何个人、团体和组织（引自ISO/IEC Guide 73）。

1.6.17. 策略

组织发展的整体计划，描述组织在将来活动中支持资源的有效利用。涉及设定目标和建议初始活动。

1.6.18. IT 的使用

计划、设计、开发、部署、运行、管理和应用IT，以满足业务的要求。包括对IT服务的要求，以及由内部业务部门、特定的IT服务部门、外部供应商和服务功能（如将软件作为一个服务提供）所提供的IT服务。

2. 良好的组织 IT 治理框架

2.1. 原则

本节为良好的组织IT治理定义六个原则。这些原则适用于大部分组织。

这些原则阐述指导决策的推荐行为。每个原则描述应该采取什么措施，但不说明如何、何时及由谁来实施这些原则 - 这些方面依赖于组织实施这些原则的特点。领导者应该有赖于这些适用原则。

2.1.1. 原则 1：职责

组织内的个人或团体理解和接受其与IT提供和需求相关的职责。并且这些活动的责任人，具有履行这些获的权利。

2.1.2. 原则 2：策略

组织的业务战略应考虑当前和未来IT 的容量； IT的策略计划应该满足组织当前和持续的业务战略的需要。

2.1.3. 原则 3：采购

应基于适当的和持续的分析、清晰可见的决策，并具有合理的理由确定IT的采购。这是对短期或长期的利益、机会、成本和风险是一个合适平衡。

2.1.4. 原则 4：绩效

IT应适合于支持组织的目的并提供服务，服务等级和服务质量应满足当前和将来的业务要求。

2.1.5. 原则 5：符合

IT应符合所有强制法律法规的要求。应该清晰定义方针和实际操作，并加以实施和推行。

2.1.6. 原则 6：人员行为

IT方针、实际操作和决策展示对人员行为的尊重，包括当前和发展所需的所有“过程中的人员”。

2.2. Model 模型

领导者应该通过三项主要任务治理IT：

a) 评估现在和将来对IT的利用。

b) 领导准备和实施计划和方针的，以保证IT的利用符合业务目标。

c) 监视方针的符合性，以及对应计划的实际绩效

图1展示了IT治理的评估-领导-监视的循环模型。图后的文件对要素和相互之间的关系进行了解释。

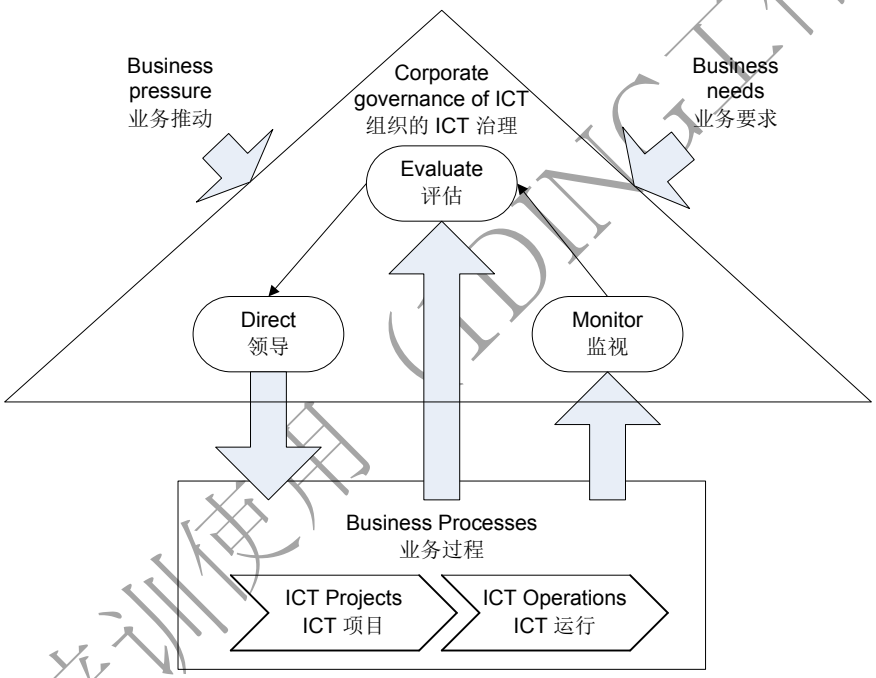

图1 组织的IT治理模型

评估

领导者应该检查和评判当前和将来对IT的利用，包括策略、建议和供给安排（不管是内部、外部，还是两者都有）。

在评估IT的使用时，领导者应该考虑对于业务的内外部压力，如技术的变更、经济和社会的发展、以及政治影响。

领导者应该随着压力的变化，持续评估。

领导者还应该考虑现在和将来的业务需求 – 当前和将来的组织必须达到的目标，如维持竞争优势，以及正在评估中的战略或意图的特定目标。

领导

领导者应该安排计划和方针的准备和实施的职责，并予以领导。计划应该设定IT项目和IT运作的投资方向。方针应该确定IT利用健全大行为。

领导者应该保证从项目转到日程运作得到了计划和管理，并考虑对业务和现有IT系统和基础设施运作习惯的影响。

领导者应该通过要求管理者提供及时的信息、符合组织的指导以及符合良好治理的六项原则，来鼓励组织内良好IT治理的文化。

如果需要，领导者应该领导所提交的建议方案的批准，以处理已识别的要求。

监视

领导者应该通过合适的测量体系监视IT的绩效。他们应该确保遵循计划，特别是与业务目标相关的。

领导者应该确保IT符合外部义务（法律、法规以及合同）和内部实际工作的要求。

注：IT特定方面的责任可能委托给组织内的管理人员。但领导者仍需为组织的IT有效和可接受的使用及交付承担责任，而不能委托。

3. 组织 IT 治理指南

3.1. 总则

以下章节提供有关良好IT治理一般原则的指南和实施这些原则所需的实践。

这里所描述的实践可能不是全面的，但提供了讨论IT治理领导人职责的起点。也就是说，这里所描述的实践是IT治理的建议指南。

充分考虑组织的特性，IT使用的适当的风险和机会分析，以识别原则的实施所需的特别行动，是每个组织自身的职责。

作为基础性说明，这里描述的实践适用于多数组织（大型的或小型的），多数情形。当然，应该考虑任何变化。

3.2. 原则 1: 职责

评估

领导者应该在组织当前和将来对IT使用的基础上，评估职责分配方案。在评估方案时，领导者应该设法确保有效、高效和可以接受的使用和交付IT，以支持当前和未来的业务目标。

领导者应该评估分配有IT决策责任的人员的能力。一般来说，这些人员应该是业务管理人员，负责组织的业务目标和绩效，并得到理解组织业务价值和过程的IT专家的协助。

领导

领导者应该领导计划按照所分配的IT职责得以执行。

领导者应该领导相关人员获得履行其职责和责任的所需信息。

监视

领导者应该监视合适的IT治理机制是否得到了建立。

领导者应该监视那些分配有职责的人员，接受和理解他们的职责。

领导者应该监视分配有IT治理职责的人员（如，在督导委员的人员或向董事会提交建议的人员）的绩效。

3.3. 原则 2：策略

评估

领导者应该评估IT和业务过程的开发，以确保IT为将来的业务要求提供支持。

在考虑计划和方针时，领导者应该评估IT活动，以确保其在不断变化的环境下与组织的目标相一致，并考虑更好的实现方式以及其他关键利益相关方的要求。

领导者应该确保IT的使用，得到了按照相关国际或国内标准所建议方式进行了风险评价和评估。

领导

领导者应该领导计划和方针的准备和适用，以确保组织从IT开发中获益。

领导者还应该鼓励IT适用的创新性建议，使得组织可以应对新的机会或挑战、承担新的业务或改进过程。

监视

领导者应该监视已获得批准的IT方案的进展，以保证其利用所分配的资源、在要求的时间框架内达到目标。

领导者应该监视IT的使用，以保证其达到预期的收益。

3.4. 原则 3：采购

评估

领导者应该评估已批准建议的IT实现方案，平衡风险和物有所值的投资建议。

领导

领导者应该管理通过合适方式获得的IT资产（系统和基础设施），包括准备合适的文件，以确保提

供所需的容量。

领导者应该领导供给安排（包括内部和外部的供给安排）以支持组织的业务要求。

监视

领导者应该监视IT投资，以保证其提供所需的容量。

领导者应该监视组织在作出任何IT采购决策时，组织和供应商共同理解组织意图的程度。

3.5. 原则 4：绩效

评估

领导者应该评估管理者所建议的方式，以保证IT具备支持业务过程所需的能力和容量。

这些建议应该处理持续日常运作的业务和处理与使用IT的相关风险。

领导者应该评估由IT活动所带来的业务持续运作的风险。

领导者应该评估信息完整性的风险和对IT资产的保护，包括相关知识产权和组织信息。

领导者应该评估有关使用IT支持业务目标的即时、有效的决策方案。

领导者应该定期评估组织IT治理体系的有效性和绩效。

领导

领导者应该按照商定的优先级和预算，分配足够的资源，以保证IT满足组织的要求。

领导者应该领导责任者，以保证IT对业务的支持。当因业务原因需要时，维护准确、不断更新的数据免受损害或误用。

监视

领导者应该监视IT对业务的支持程度。

领导者应该监视所分配的资源和预算优先次序与业务目标吻合的程度。

领导者应该监视方针恰当性的程度，如数据的准确性和IT利用的效率。

3.6. 原则 5：符合

评估

领导者应该定期评估IT满足义务（法律法规、合同）、内部方针、标准和专业指南的程度。

领导者应该定期评估组织内部对其自身的IT治理体系的符合性。

领导

领导者应该领导责任人，建立定期和例行机制以保证IT的使用符合相关义务（法律法规、合同）、标准和专业指南

领导者应该领导方针的建立和推行，以保证组织的IT使用符合其内部义务。

领导者应该领导IT员工遵循相关专业行为和开发的指南。

领导者应该领导所有IT相关活动合乎伦理道德。

监视

领导者应该通过合适的报告和审计活动，监视IT的符合性和一致性，以确保评审对于评估业务得到满足的程度是及时、全面和适宜。

领导者应该监视IT活动，包括资产和数据的废弃，以保证环境、隐私、战略知识管理、组织私有技术和其它相关义务得到满足。

3.7. 原则 6：人员行为

评估

领导者应该评估IT活动，以确保对人员行为的识别和考虑。

领导

领导者应该领导IT活动义识别的人员行为的一致性。

领导者应该管理由任何人在任何时间报告或识别的风险、机会、问题和关心事项。风险的管理应该按照已发布的策略和程序，并升级到相关决策者。

监视

领导者应该监视IT活动以保证，以确保已识别的人员行为仍然有关，并且已采取适当注意。

领导者应该监视实际工作方式，以保证其与合理使用IT的一致性。