

INTERNATIONAL STANDARD

ISO/IEC 19770-1

Third edition
2017-12

Information technology — IT asset management —

Part 1: IT asset management systems — Requirements

*Technologies de l'information — Gestion des actifs logiciels —
Partie 1: Procédés et évaluation progressive de la conformité*



Reference number
ISO/IEC 19770-1:2017(E)

© ISO/IEC 2017

奥邦检验认证集团

奥邦检验认证集团公示用途

奥邦检验认证集团公示用途



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
1.1 Purpose	1
1.2 Field of application	1
1.3 Limitations	1
2 Normative references	2
3 Terms and definitions	2
4 Context of the organization	12
4.1 Understanding the organization and its context	12
4.2 Understanding the needs and expectations of stakeholders	12
4.3 Determining the scope of the IT asset management system	13
4.4 IT asset management system	13
5 Leadership	13
5.1 Leadership and commitment	13
5.2 Policy	14
5.3 Organizational roles, responsibilities and authorities	14
6 Planning	15
6.1 Actions to address risks and opportunities for the IT asset management system	15
6.1.1 General	15
6.1.2 IT asset risk assessment	15
6.1.3 IT asset risk treatment	16
6.2 IT asset management objectives and planning to achieve them	16
6.2.1 IT asset management operation process specification	16
6.2.2 IT asset management objectives for operation processes	17
6.2.3 Overall IT asset management objectives	17
6.2.4 Planning to achieve IT asset management objectives	17
7 Support	18
7.1 Resources	18
7.2 Competence	18
7.3 Awareness	19
7.4 Communication	19
7.5 Information requirements	19
7.6 Documented information	20
7.6.1 General	20
7.6.2 Traceability of ownership and responsibility	20
7.6.3 Audit trails of authorizations and execution of authorizations	21
7.6.4 Creating and updating	21
7.6.5 Control of documented information	21
8 Operation	22
8.1 Operational planning and control	22
8.2 Management of change	22
8.3 Core data management	22
8.4 License management	22
8.5 Security management	23
8.6 Other processes	23
8.7 Outsourcing and services	23
8.8 Mixed responsibilities between the organization and its personnel	24
9 Performance evaluation	24
9.1 Monitoring, measurement, analysis and evaluation	24
9.2 Internal audit	25

9.3 Management review..... 25

10 Improvement..... 26

10.1 Nonconformity and corrective action..... 26

10.2 Preventive action..... 26

10.3 Continual improvement..... 26

Annex A (normative) IT asset management operation processes and objectives 27

Annex B (informative) IT asset management tiers 31

Annex C (informative) Characteristics of IT Assets 33

Annex D (informative) Changes from ISO 55001 35

Bibliography 37

国际标准

ISO/IEC
19770-1

2017 年 12 月
第三版

信息技术 - IT 资产管理 -

第 1 部分 IT 资产管理体系 - 要求

信息技术 - IT 资产管理 - 第 1 部分

奥邦检验认证集团有限公司翻译
内部资料 严谨外传



Reference number
ISO/IEC 19770-1:2017(E)

©ISO/IEC 2017



受版权保护的文件

©ISO/IEC 2017, 瑞士出版

版权所有。除非另有规定，未经事先书面许可，不得以任何形式或任何手段（电子或机械手段，包括复印或在互联网或内联网上发布）复制或以其他方式使用本出版物的任何部分。可向 ISO 下列地址或 ISO 在所在国的成员机构提出许可申请。

国际标准化组织版

权办公室

瑞士日内瓦韦尔尼耶市布兰东内街

8 号，邮编 1214 电话：+41 22

749 01 1 传真：+41 22 749 09

47 邮箱：copyright@iso.org 网

址：www.iso.org

目录

前言	4
信息技术 - IT 资产管理 -	8
第一部分 IT 资产管理体系 - 要求	8
1 范围	8
1.1 目的	8
1.2 应用范围	8
1.3 限制	8
2 规范性引用文件	9
3 术语和定义	9
4 组织的背景	20
4.1 了解组织及其背景	20
4.2 了解利益相关方的需求和期望	20
4.3 确定信息技术资产管理体系范围	20
4.4 IT 资产管理体系	20
5 领导作用	21
5.1 领导作用与承诺	21
5.2 方针	21
5.3 组织的岗位、职责与权限	22
6 策划	22
6.1 为 IT 资产管理体系应对风险和机遇所采取的措施	22
6.2 IT 资产管理目标及实现这些目标的规划	23
7 支持	25
7.1 资源	25
7.2 能力	25
7.3 意识	25
7.4 沟通	25
7.5 信息需求	26
7.6 文档化信息	26
8 运行	28
8.1 运行策划与控制	28
8.2 变更管理	28
8.3 核心数据管理	28
8.4 许可证管理	28
8.5 安全管理	28
8.6 其他流程	29
8.7 外包与服务	29
8.8 组织与员工在 IT 资产及所存储信息方面的共同责任	29
9 绩效评价	30
9.1 监控、测量、分析与评价	30
9.2 内部审核	31
10 改进	31
10.1 不合格与纠正措施	31
10.2 预防措施	32
10.3 持续改进	32
附件 A:	33
附件 B:	37
附件 C:	39
附录 D:	40

前言

国际标准化组织（ISO）和国际电工委员会（IEC）构成了全球标准化的专业体系。作为 ISO 或 IEC 成员的各国机构通过各自组织为处理特定技术领域而设立的技术委员会参与国际标准的制定。ISO 和 IEC 的技术委员会在共同感兴趣的领域开展合作。其他国际组织，无论是政府的还是非政府的，在与 ISO 和 IEC 联络的情况下也参与相关工作。在信息技术领域，ISO 和 IEC 成立了一个联合技术委员会，即 ISO/IEC JTC 1。

本文件的编制程序以及其后续维护所采用的程序在 ISO/IEC 指令第 1 部分中有描述。尤其应注意不同类型的文件所需的不同批准标准。本文件是依照 ISO/IEC 指令第 2 部分的编辑规则起草的（见 www.iso.org/directives）。

请注意，本文件中的某些元素可能受专利权保护。国际标准化组织（ISO）和国际电工委员会（IEC）不对识别任何此类专利权负责。在文件编制过程中识别出的任何专利权详情将在引言部分和/或国际标准化组织收到的专利声明清单中列出（见 www.iso.org/patents）。

本文件中使用的任何商标名称均为方便用户而提供，不构成认可。

有关标准自愿性的说明、与合格评定相关的 ISO 特定术语和表达的含义，以及 ISO 遵守世界贸易组织（WTO）技术性贸易壁垒（TBT）原则的信息，请访问以下网址：

www.iso.org/iso/foreword.html。

本文件由国际标准化组织/国际电工委员会联合技术委员会 ISO/IEC JTC 1 信息技术分技术委员会 SC 7 软件和系统工程编制。特别邀请了 ISO/IEC JTC 1/SC 27 信息技术安全技术、ISO/IEC JTC 1/SC 40 信息技术服务管理和信息技术治理以及 ISO/TC 251 资产管理参与并作出贡献。

本第三版废止并取代了第二版（ISO/IEC 19770-1:2012），该版本在技术上进行了修订，成为一项管理体系标准。

国际标准化组织（ISO）网站上列有 ISO/IEC 19770 系列的所有部分。

引言

本文件规定了信息技术资产管理（ITAM）管理体系（简称“IT 资产管理体系”）的建立、实施、保持和改进的要求。

本文件为 ISO 55001:2014 提供了补充要求，该标准规定了建立、实施、保持和改进资产管理管理体系（简称“资产管理体系”）的要求。本文件包含了被认为对 IT 资产管理必要的额外或更详细的要求。主要的区别在于需要管理具有特定特征的软件资产。尽管如果组织恰当地定义其范围和相关要求，ISO 55001:2014 可用于管理软件资产，但它主要侧重于实物资产，对软件资产的管理规定较少。

信息技术资产具有一些特性，这些特性导致了额外或更详细的要求。这些特性在附录 C 中进行了描述。由于信息技术资产的这些特性，信息技术资产的管理体系将因此具有除 ISO 55001:2014 中的要求之外的明确要求，涉及以下方面：

- 对软件修改、复制和分发的控制，尤其要注重访问和完整性控制；
- 对信息技术资产授权和变更的审核追踪；
- 对许可、许可不足、许可过度以及对许可条款和条件的遵守情况的控制；
- 对涉及混合所有权和责任的情况的控制，例如在云计算和“自带设备”（BYOD）实践中；
- 当业务价值合理时，信息技术资产管理数据与其他信息系统（特别是记录资产和费用的财务信息系统）数据的核对。

此外，由于与 IT 资产相关的信息通常数量庞大、高度复杂且变化迅速，拥有此类信息的组织很可能需要利用自动化信息系统。

ISO 55001:2014 与本文件的另一个区别在于，本文件可选择性地为多个明确的流程目标分组（或称为“层级”）提供支持。其中最重要的是被称为“可信数据”的基本层级，这对大多数终端用户组织和软件发行商来说最为重要。第二层级是“生命周期集成”，第三层级是“优化”。关于各层级及其各自的目标分组的更多信息，请参见附录 B。

由于主要的实物资产越来越多地融入或依赖软件，因此在这种情况下，本文件中的附加要求很可能适用。大多数拥有主要实物资产的组织很可能需要满足 ISO 55001:2014 中“纯粹”的要求以及本文件中附加要求的混合管理体系。

IT 资产涵盖多种资产类型。图 1 以图表形式展示了主要的 IT 资产类型。

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1) 通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2) 也可通过客服电话咨询 **025-85307007**。