ICS 03.100.01
CCS A 01

DB6101

西　　安　　市　　地　　方　　标　　准

DB 6101/T 3232—2025

科技型中小企业商业秘密管理体系 要求

2025－03－15 发布　　2025－04－15 实施

西安市市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由西安交通大学提出。

本文件由西安市市场监督管理局归口。

本文件起草单位：西安交通大学、西安市质量与标准化研究院、西安市知识产权保护中心、西安市中级人民法院西安知识产权法庭、西安市公证处、陕西省技术经理人协会、中知（北京）认证有限公司、陕西众森电能科技有限公司、陕西软唐知识产权代理事务所（特殊普通合伙）、西安政合企业管理咨询有限公司。

本文件主要起草人：孙那、李春政、马兰、李铨、王泉、王黎、王凯、余平、冉旭、李鑫、李飞、赵佳、陈逸飞、杨帆、张鹤仙、张小丹、郭秉印、鲍一鸣。

本文件由西安交通大学负责解释。

本文件首次发布。

本文件在实施中如有疑问或建议，请将咨询或修改建议反馈至下列单位：

单位：西安交通大学

地址：陕西省西安市碑林区咸宁西路28号西安交通大学（兴庆校区）

电话：029-82665824

邮编：710048

引　言

0.1 总则

本文件旨在帮助科技型中小企业建立和完善商业秘密管理体系，防止商业秘密泄露或者掌握核心重要商业秘密的人才流失给企业造成损失，帮助企业在商业秘密泄露造成损失后能够有效寻求法律救济，维护企业合法权益，促进企业的健康发展。

0.2 基本理念

0.2.1 需求导向

科技型中小企业可按照本文件进行企业商业秘密管理体系的设计，也可在本文件的基础上，根据企业实际进行创新设计，构建系统、协调、适应企业发展战略和经营管理需要的企业商业秘密管理体系。

0.2.2 系统管理

运用系统管理的原理和方法，识别企业生产、经营、管理全过程中相互关联、相互作用的要素，建立商业秘密管理体系，并与企业经营管理系统充分融合、相互协调，发挥系统效应，提高企业实现目标的有效性。

0.2.3 持续改进

采用“PDCA(策划—实施—检查—处置)”的循环管理模式，实现科技型中小企业商业秘密管理体系的持续改进。

0.3 模型图

以商业秘密管理需求为导向，构建商业秘密管理体系，并遵循“PDCA”理念和方法，实现系统管理和持续改进。商业秘密管理系统模型如图1所示。

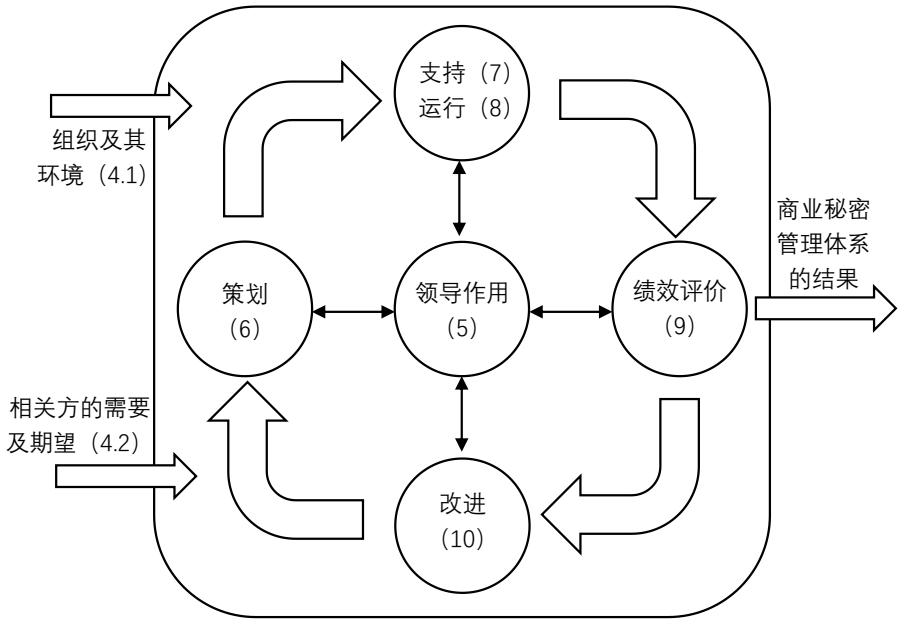

图1　基于过程管理的商业秘密管理模型

0.4 与其他管理体系的关系

本文件采用ISO制定的管理体系标准框架（HLS），以提高与其他管理体系标准的协调一致性。

本文件遵循商业秘密管理思路，提出企业商业秘密管理体系的要求，指导企业策划、实施和运行、评审和改进商业秘密管理体系。

科技型中小企业商业秘密管理体系 要求

1 范围

本文件规定了科技型中小企业商业秘密管理体系组织环境、领导作用、策划、支持、运行、绩效评价和改进的要求。

本文件适用于科技型中小企业商业秘密管理体系的构建。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 19000 质量管理体系 基础和术语

3 术语和定义

GB/T 19000界定的以及下列术语和定义适用于本文件。

3.1

科技型中小企业

依托一定数量的科技人员从事科学技术研究开发活动，取得自主知识产权并将其转化为高新技术产品或服务，从而实现可持续发展的中小企业。

3.2

商业秘密

不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息和经营信息等商业信息。

3.3

管理体系

组织为确立方针和目标以及实现这些目标的过程所形成的相互关联或相互作用的一组要件。

注1：一个管理体系可能针对一个或几个主题。

注2：管理体系要件包括组织的结构、岗位和职责、策划和运行。

[来源：GB/T 19000，3.5.3，有修改]

3.4

最高管理者

在最高层指挥和控制组织的一个人或一组人。

注1：最高管理者有权在组织内部授权和提供资源。

注2：如果管理体系（3.3）的范围仅覆盖组织的某个组成部分，那么最高管理者是指挥和控制该部分的一个人或一组人。

[来源：GB/T 19000，3.1.1，有修改]

3.5 **相关方**

那些能够影响决策或活动、受决策或活动影响或自认为受决策或活动影响的个人或组织。

［来源：GB/T 19000，3.2.3，有修改］

3.6

文件化信息

需要控制和维护的信息载体。

注1：文件化信息能够以任何形式和载体存在，且来源不限。

注2：文件化信息可能涉及：

［来源：GB/T 19000，3.8.6，有修改］

3.7

商业秘密管理绩效

在商业秘密管理方面可测量的结果。

4 组织环境

4.1 组织及环境

组织应确定与其宗旨相关的，并影响其实现商业秘密管理体系预期结果的能力的内部和外部事项，包括但不限于：

——社会、文化、环境背景；

——经济状况；

——法律和监管环境；

——业务模式，包括组织活动和运行的战略、性质、规模、复杂性和可持续性；

——与第三方业务关系的性质和范围；

——内部结构、方针、过程、程序和资源；

——应采取保密措施的技术信息和经营信息等商业信息。

4.2 理解相关方的需要和期望

组织应确定：

——与商业秘密管理体系有关的相关方；

注：相关方可包括商业秘密权利人、员工、顾客、供方、合作伙伴、竞争对手、国家机关等。

——与商业秘密管理体系有关的相关方的需求；

注：需求可包括组织规章制度、合同协议、法律法规的要求。

——组织应监视和评审这些相关方的信息及其相关需求，判定哪些需求将通过商业秘密管理体系予以解决。

4.3 确定商业秘密管理体系的范围

4.3.1 组织应确定商业秘密管理体系的边界和适用性，以确立其范围。

4.3.2 组织应根据以下内容确定商业秘密管理体系的范围：

——4.1 提及的内部和外部事项；

——4.2 提及的需求；

——商业秘密管理需求；

——组织的技术信息和经营信息等商业信息。

4.3.3 组织商业秘密管理体系应包括在组织控制下或在其影响范围内可能影响组织商业秘密管理绩效的活动、产品和服务。

4.3.4　范围应作为文件化信息可获取。

4.4　商业秘密管理体系

4.4.1　组织根据本文件的要求，应建立、实施、维护和持续改进商业秘密管理体系，包括所需的过程及相互作用。

4.4.2　组织应确定商业秘密管理体系所需的过程及其在整个组织中的应用，且应：

——确定这些过程所需的输入和期望的输出；

——确定这些过程的顺序和相互作用；

——确定和应用所需的准则和方法（包括监视、测量和相关绩效指标），以确保这些过程的有效运行和控制；

——确定这些过程所需的资源并确保可获得；

——分配这些过程的职责和权限；

——按照 6.1 的要求应对风险和机遇；

——评价这些过程，实施所需的变更，以确保实现这些过程的预期结果；

——确保过程和商业秘密管理体系持续改进。

4.4.3　在必要的范围和程度上，组织应：

——保持文件化信息以支持过程运行；

——保留文件化信息以确信其过程按策划进行。

5　领导作用

5.1　领导作用和承诺

最高管理者应通过以下方面证实其对商业秘密管理体系的领导作用和承诺：

——对商业秘密管理体系的有效性负责；

——确保商业秘密方针和商业秘密目标得以确立，并与组织环境相适应，与组织的战略方向一致；

——确保将商业秘密管理体系要求融入组织的业务过程；

——促进使用过程方法和基于风险的思维；

——确保商业秘密管理体系所需的资源可获取；

——就有效的商业秘密管理的重要性以及符合商业秘密管理体系要求的重要性进行沟通；

——确保商业秘密管理体系实现其预期结果；

——指导和支持人员为商业秘密管理体系的有效性做出贡献；

——促进持续改进；

——支持其他相关岗位在职责范围内证实其领导作用。

5.2　商业秘密管理文化

5.2.1　组织应建立文化培育机制，将商业秘密保护意识融入组织价值观和日常行为准则，形成全员参与、主动防范的文化氛围。

5.2.2　最高管理者和管理者应证实，对于整个组织所要求的商业秘密共同行为准则，其做出了积极的、明示的、一致且持续的承诺。

5.2.3　组织应在其内部各个层级建立、维护并推进商业秘密管理文化。

注1：战略层——将商业秘密保护纳入企业战略目标，与创新文化、合规文化协同推进；

注2：管理层——通过制度设计（如绩效考核、奖惩机制）将商业秘密保护要求嵌入业务流程；

注3：执行层——针对研发、销售、供应链等不同岗位，制定差异化的商业秘密保护行为指引和培训内容。

5.2.4 组织应通过典型案例分析（如内部泄密事件模拟、行业标杆实践）强化员工风险感知，利用数字化工具（如企业知识库、在线培训平台）实现商业秘密管理文化的常态化宣贯。

5.2.5 组织应开展商业秘密管理文化建设评估工作，动态调整文化培育策略。

5.2.6 组织应鼓励全员通过内部沟通渠道、创新提案等方式参与商业秘密管理文化改进。

5.2.7 组织应与合作伙伴、供应商的合同中明确商业秘密管理义务，传递商业秘密管理文化。

5.3 商业秘密管理方针

5.3.1 最高管理者应确立商业秘密管理方针，方针应：

——适应于组织的宗旨和环境；

——为设定商业秘密管理目标提供框架；

——包括满足适用需求的承诺；

——包括持续改进商业秘密管理体系的承诺。

5.3.2 商业秘密管理方针应：

——作为文件化信息可获取；

——在组织内予以沟通；

——视情况，可被相关方获取。

5.4 岗位、职责和权限

5.4.1 最高管理者

最高管理者应确保在组织内部分配并沟通相关岗位的职责和权限。

最高管理者应：

——为建立、制定、实施、评价、维护和改进商业秘密管理体系配置足够且适当的资源；

——确保建立及时有效的商业秘密管理绩效报告制度；

——确保战略和运行目标与商业秘密管理目标相协同；

——确立和维护问责机制，包括纪律处分和结果；

——确保商业秘密管理绩效和人员绩效考核挂钩。

5.4.2 商业秘密管理机构

应明确商业秘密管理机构，并配备专业的专职或兼职工作人员，承担以下职责：

——推进识别商业秘密管理目标，监督已识别的商业秘密管理目标的职责在组织内得到适当分配；

——负责就商业秘密相关事项提出建议；

——负责组织商业秘密日常管理工作，包括但不限于文件管理、工作计划制定和实施、监督和考核完成情况；

——负责统筹与其他管理机构相关的商业秘密管理工作。

5.4.3 管理者

管理者应负责：

——配合和支持管理机构；

——确保在其控制下的所有人员都遵守组织的商业秘密管理方针、目标、程序；

——识别其运行中的商业秘密活动并进行沟通；

注：商业秘密活动包含但不限于：商业秘密的产生、识别、接收、保密、披露、公开、救济。

——在其职责范围内将商业秘密管理目标融入现有的业务实践和程序；
——参加并协助商业秘密培训活动；
——培养人员的商业秘密意识，指导他们满足 7.2 的要求；
——鼓励并支持人员提出商业秘密管理疑虑，并防止其遭到任何形式的报复；
——根据要求积极参与商业秘密相关事件和事项的管理、解决；
——确认需要采取纠正措施时，适当的纠正措施能得到推荐和实施。

6 策划

6.1 应对风险和机遇的措施

6.1.1 在策划商业秘密管理体系时，组织应根据 4.1 提及的因素、4.2 提及的需求和 4.3 提及的范围，并确定需要应对的风险和机遇：
——确保商业秘密管理体系能够实现预期结果；
——把握机遇；
——预防或减少不利影响；
——实现持续改进。

6.1.2 组织应策划：
——应对这些风险和机遇的措施；
——如何将措施纳入商业秘密管理体系过程并实施且评价这些措施的有效性。

6.2 商业秘密管理目标及其实现的策划

6.2.1 组织应在相关职能和层级上确立商业秘密管理目标，并应：
——与商业秘密管理方针一致；
——可测量(如果可行)；
——体现适用的需求；
——予以监视；
——予以沟通；
——视情况予以更新；
——作为文件化信息可获取。

6.2.2 策划如何实现商业秘密管理目标时，组织应确定：
——要做什么；
——需要什么资源；
——由谁负责；
——何地、何时完成；
——如何评价结果。

6.3 针对变更的策划

当组织确定需要变更商业秘密管理体系时，应对这些变更的实施进行策划。
组织应结合：
——变更目的及其潜在后果；
——商业秘密管理体系设计和运行的有效性；
——足够资源的可获取性；

——职责和权限的分配或再分配。

7 支持

7.1 资源

7.1.1 总则

组织应确定并提供所需的资源，以建立、实施、保持和持续改进商业秘密管理体系，应结合：

——现有内部资源的能力和局限，比如应当考虑是否具备胜任商业秘密管理的人员、是否可招聘到商业秘密管理人员以及建立商业秘密管理体系的最低成本；

——需要从外部获得的资源，比如擅长商业秘密管理的外部专家。

7.1.2 人员

组织应确定相关岗位及职责，并配备所需的人员，以有效实施商业秘密管理体系，并运行和控制其过程。包括：

——所有人员应履行商业秘密管理职责，并报告商业秘密管理疑虑、问题和漏洞；

——对拟聘任人员进行适当的背景调查，必要时可签署相关声明文件；

——通过劳动合同、劳务合同或者单独签订保密协议等方式对人员进行管理，约定保密范围、保密义务、违约责任等，明确人员与商业秘密管理相关的权利和义务，应与高级管理人员、高级技术人员和其他负有保密义务的人员签订竞业限制协议；

——在调动和晋升之前，组织应结合岗位和人员可能引发的商业秘密管理风险，进行尽职调查；

——对离退人员应进行商业秘密事项提醒，必要时对保密协议或竞业限制协议的执行情况进行监视；

——明确人员在商业秘密活动中的奖惩条件和标准，对于违反组织商业秘密管理要求、方针、过程和程序的人员，应追究相应的责任。

7.1.3 基础设施

组织应确定、提供并维护所需的基础设施，以确保商业秘密管理体系的运行。基础设施包括但不限于：

——软件、硬件，如商业秘密管理软件、数据库、访客管理系统、计算机、专用存储介质、监控设备、保险柜、网络设施等；

——办公场所。

7.1.4 财务资源

组织确定并提供财务资源，以有效实施商业秘密管理体系。财务资源可用于：

——商业秘密管理活动；

——商业秘密管理机构运行；

——商业秘密活动的激励；

——商业秘密维权。

7.2 能力

7.2.1 总则

组织应：

——确定在其控制下工作、影响商业秘密管理绩效的人员所需的能力；

——确保这些人员在适当的教育、培训或经验的基础上胜任工作；

——适用时，采取措施获得所需的能力，并评价所采取措施的有效性；

——适当的文件化信息应作为能力证据可获取。

注：适当的措施可能包括，例如：向现有人员提供培训、指导或重新分配工作；或者聘用能够胜任的专职或兼职人员。

7.2.2 培训

7.2.2.1 组织应对全员进行培训，培训应在聘用开始时和组织策划的时间间隔实施。培训应：

——适合于人员的岗位及其面临的商业秘密管理风险；

——进行有效性评估，如问卷测评、访谈、演示等；

——进行评审。

7.2.2.2 结合已识别的商业秘密管理风险，组织应确保实施程序对代表组织开展业务并可能给组织带来商业秘密管理风险的第三方进行培训，提高其商业秘密管理意识。

7.2.2.3 培训记录应作为文件化信息予以保留。

7.3 意识

在组织控制下工作的人员应知道：

——商业秘密方针；

——他们对商业秘密管理体系有效性的贡献，包括改善商业秘密管理绩效带来的效益；

——不符合商业秘密管理体系要求的后果；

——提出商业秘密管理疑虑的方法和程序；

——工作岗位的商业秘密管理要求与商业秘密方针的关系；

——支持商业秘密文化的重要性。

7.4 沟通

7.4.1 组织应确定与商业秘密管理体系有关的内部和外部沟通，包括：

——沟通什么；

——何时沟通；

——与谁沟通；

——由谁沟通；

——如何沟通。

7.4.2 组织应：

——结合沟通需求，综合考虑沟通的多样性和潜在障碍；

——确立沟通的过程，确保结合了相关方的意见；

——在确立沟通过程时：

- 应将其商业秘密管理文化、商业秘密管理目标纳入沟通内容；
- 应确保所沟通的商业秘密相关信息与来源于商业秘密管理体系的信息一致且可信。

——对与商业秘密管理体系相关的沟通内容进行回应；

——保留文件化信息作为其沟通的证据；

——在组织的各层级和职能内部沟通与商业秘密管理体系有关的信息，视情况包括商业秘密管理体系的变更；

——确保人员能在沟通过程中为商业秘密管理体系的持续改进做出贡献；
——确保人员能在沟通过程中提出商业秘密管理疑虑；
——通过组织确立的沟通过程对外沟通，包括其商业秘密文化、商业秘密管理目标在内的与商业秘密管理体系相关的信息。

7.5 文件化信息

7.5.1 总则

组织的商业秘密管理体系应包括：
——本文件要求的文件化信息；
——组织确定的，对于商业秘密管理体系有效性所必需的文件化信息。

注：不同组织的商业秘密管理体系文件化信息的程度可能不同，取决于：

- 组织的规模及其活动、过程、产品和服务的类型；
- 过程及其相互作用的复杂度；
- 人员的能力。

7.5.2 文件化信息的创建和更新

在创建和更新文件化信息时，组织应确保适当的：
——标记和说明(例如，标题、日期、作者或文件编号)；
——形式(例如，语言文字、软件版本、图形)和载体(例如纸质的、电子的)；
——针对适宜性和充分性的评审和批准；
——信息化管理和记录管理。

7.5.3 文件化信息的控制

7.5.3.1 应控制商业秘密管理体系和本文件要求的文件化信息，以确保其：
——在需要的场所和时间均可获得并适于使用；
——得到充分保护(例如，防止泄密、不当使用或完整性受损)。

7.5.3.2 为了控制文件化信息，组织应开展以下适用的活动：
——分发、访问、检索和使用；
——存储和防护，包括保持易读性；
——对变更的控制(例如，版本控制)；
——保留和处置。

7.5.3.3 对于组织确定的、策划和运行商业秘密管理体系必要的、来自外部的文件化信息，应视情况进行识别，并予以控制。

注：访问可能意味着只允许查看文件化信息的权限，或者允许并授权查看和变更文件化信息的权限。

8 运行

8.1 策划和控制

8.1.1 为满足商业秘密管理体系的要求，并实施第 6 章所确定的措施，组织应通过以下措施对所需的过程进行策划、实施和控制：
——确定商业秘密管理要求；
——建立商业秘密管理过程准则；

——确定所需的资源；
——按照准则实施过程控制；
——在必要的范围和程度上，保留策划和控制过程的文件化信息，以确保过程已经按策划进行。

8.1.2 组织应确保对外部提供的与商业秘密管理体系相关的产品、过程或服务实施控制。

8.1.3 组织应控制策划的变更，评审非预期变更的后果，必要时，采取措施减轻不利影响。

8.2 商业秘密的管理

组织应按照 8.1 的要求开展商业秘密的管理工作，包括但不限于：
——识别和确定商业秘密；
——采取措施保护商业秘密；
——根据需要变更商业秘密；
——解除不具有保密价值或由于特定因素导致被公开的商业秘密；
——销毁不需留存的商业秘密；
——组织应定期对商业秘密管理措施进行评审。

8.3 涉密事项的管理

组织应按照 8.1 的要求开展涉密事项的管理工作，并保留适当的文件化信息,包括但不限于：
——识别和确定涉密事项(如涉密人员、涉密信息、涉密等级、涉密载体、涉密物品、涉密区域、涉密活动等)；
——确定各涉密事项的管理过程或对象；
——制定各涉密事项的管理措施；
——实施涉密事项的过程管理；
——组织应定期对涉密事项管理措施进行评审。

8.4 应急准备及响应

8.4.1 应急准备

为了对 6.1 中所识别的潜在紧急情况进行应急准备，组织应建立、实施并保持所需的过程，包括：
——针对涉密载体丢失、商业秘密泄露、侵权、违约等紧急情况策划应急预案；
——为所策划的响应提供支持；
——定期对策划的应急预案进行测试或演练；
——定期评审并修订过程和策划的响应措施，特别是发生紧急情况后或进行测试或演练后；
——组织应保留关于响应潜在紧急情况的过程和计划的文件化信息。

8.4.2 应急响应

组织应对已发生或疑似发生的泄密、侵权等紧急情况做出响应，包括但不限于：
——启动对商业秘密泄露、侵权等紧急事件的核查，控制并降低紧急情况引发的影响或损失，确认事件发生的事实和过程；
——分析商业秘密泄露或侵权原因，并评估事件的严重程度；
——收集和固定相关证据；必要时，可委托律师调查取证、通过公证机构取证、向法院申请证据保全和申请法院调查取证；
——依法开展维权，向市场监督管理部门、公安机关、人民法院等寻求行政保护和司法保护；
——评估紧急情况对相关方的影响，采取相应措施并与相关方沟通。

9 绩效评价

9.1 监视、测量、分析和评价

9.1.1 组织应建立，实施和保持用于监视、测量、分析和评价商业秘密管理绩效的过程。组织应确定：

——需要监视和测量的内容；

——适用的监视测量、分析和评价的方法，以确保有效的结果；

——何时实施监视和测量；

——何时对监视和测量的结果进行分析和评价。

9.1.2 文件化信息应作为过程和结果证据可获取。

9.1.3 组织应评价商业秘密管理体系的绩效和有效性。

9.2 内部审核

9.2.1 总则

组织应在策划的时间间隔内实施内部审核，以便为商业秘密管理体系提供以下信息：

——是否符合：

- 组织自身对商业秘密管理体系的要求；
- 本文件的要求。

——是否得到了有效地实施和维护。

9.2.2 内部审核方案

9.2.2.1 组织应策划、确立、实施和维护审核方案，包括频次、方法、职责、策划要求和报告。

9.2.2.2 组织应根据相关过程的重要性和以往审核的结果，确立内部审核方案。

9.2.2.3 组织应：

——界定每次审核的目标、准则和范围；

——选择审核员并实施审核，以确保审核过程的客观性和公正性；

——确保向相关管理者报告审核结果；

——及时采取适当的纠正和纠正措施；

——保留文件化信息，作为实施审核方案和审核结果的证据。

9.3 管理评审

9.3.1 总则

最高管理者应在策划的时间间隔内对组织的商业秘密管理体系进行评审，以确保商业秘密管理体系持续的适宜性、充分性和有效性。

9.3.2 管理评审输入

管理评审应包括：

——以往管理评审所采取措施的状况；

——与商业秘密管理体系有关的外部和内部事项的变化；

——与商业秘密管理体系有关的相关方需要和期望的变化；

——关于商业秘密管理绩效的信息，包括以下方面的趋势：

- 不符合与纠正措施；

- 监视和测量的结果；
- 审核结果。

——持续改进的机会。

9.3.3 管理评审结果

9.3.3.1 管理评审的结果应包括持续改进的机会，以及变更商业秘密管理体系的任何需要的决定。

9.3.3.2 文件化信息应作为管理评审结果证据可获取。

10 改进

10.1 不符合与纠正措施

10.1.1 发生不符合时，组织应：

——对不符合做出反应，并且：

- 采取措施以控制和纠正；
- 处置后果。

——通过以下活动评价采取措施的需要，以消除产生不符合的原因，避免其再次发生或在其他地方发生：

- 评审不符合；
- 确定产生不符合的原因；
- 确定是否存在或可能发生类似的不符合。

——实施任何所需的措施；

——评审所采取的任何纠正措施的有效性；

——如必要，变更商业秘密管理体系。

10.1.2 纠正措施应与不符合产生的影响相适应。

10.1.3 文件化信息应作为以下事项的证据可获取：

——不符合的性质和所采取的任何后续措施；

——任何纠正措施的结果。

10.2 持续改进

组织应持续改进商业秘密管理体系的适宜性、充分性和有效性。

参 考 文 献

[1] 《科技型中小企业评价办法》（国科发政〔2017〕115号）
[2] 《中华人民共和国反不正当竞争法》
[3] GB/T 19001 质量管理体系 要求
[4] GB/T 20001.11 标准编写规则 第11部分：管理体系标准
[5] GB/T 20002.6—2022 标准中特定内容的编写指南 第6部分：涉及中小微企业需求
[6] GB/T 35770-2022 合规管理体系 指南
[7] DB61/T 1429—2021 企业技术创新管理体系 要求