



# 中华人民共和国国家标准

GB/T 41207—2021/ISO 30302:2015

## 信息与文献 文件(档案)管理体系 实施指南

Information and documentation—Management systems for records—  
Guidelines for implementation

(ISO 30302:2015, IDT)

2021-12-31 发布

2022-07-01 实施

国家市场监督管理总局  
国家标准化管理委员会 发布



## 目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 组织背景	1
4.1 了解组织及其背景	1
4.2 业务、法律及其他需考虑的因素	2
4.3 界定 MSR 的范围	3
5 领导作用	3
5.1 管理承诺	3
5.2 方针	3
5.3 组织的岗位、职责和权限	4
5.3.1 总则	4
5.3.2 管理职责	5
5.3.3 执行职责	5
6 规划	6
6.1 应对风险和机遇的措施	6
6.2 文件管理的目标和规划	7
7 支持	8
7.1 资源	8
7.2 能力	8
7.3 意识和培训	9
7.4 沟通	10
7.5 证明性文档	10
7.5.1 总则	10
7.5.2 证明性文档的控制	12
8 运行	12
8.1 运行规划和控制	12
8.2 文件过程的设计	13
8.3 文件系统的实施	15
9 绩效评价	16
9.1 监控、测量、分析和评价	16

9.1.1 确定如何监控、测量、分析和评估,及其内容	16
9.1.2 对于文件过程和文件系统运行绩效,以及 MSR 有效性的评估	17
9.1.3 评估有效性	17
9.2 内部体系审计	18
9.3 管理评审	18
10 改进	19
10.1 不符合项控制和纠正措施	19
10.2 持续改进	20
附录 A (资料性) 关于信息来源和支持组织背景分析需考虑因素的示例	21
A.1 信息来源	21
A.2 需考虑的因素	21
参考文献	23

## 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。

GB/T 41207《信息与文献　文件(档案)管理体系　实施指南》、GB/T 34112《信息与文献　文件管理体系　要求》和 GB/T 34110《信息与文献　文件管理体系　基础与术语》共同构成支撑文件管理的系列国家标准。

本文件使用翻译法等同采用 ISO 30302:2015《信息与文献　文件(档案)管理体系　实施指南》。

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。

本文件由全国信息与文献标准化技术委员会(SAC/TC 4)提出并归口。

本文件起草单位:中国人民大学、国家档案局、天津师范大学、中国科学技术信息研究所、山东省计算中心(国家超级计算济南中心)、高地知库(北京)信息咨询有限公司、中电科大数据研究院有限公司、郑州航富数波科技有限公司、上海信联信息发展股份有限公司、深圳市电子政务云计算应用技术国家工程实验室有限公司。

本文件主要起草人:安小米、白文琳、聂曼影、加小双、刘春燕、蔡盈芳、钱恒、孙舒扬、王金祥、张大鹏、何芮、杨安荣、庞玲玲、胡菊芳、程序、连樟文。

## 引言

GB/T 34110 对文件(档案)管理体系(MSR)系列标准和 MSR 目标及受益和相关术语进行了详细说明;GB/T 34112 对 MSR 需考虑的因素进行了详细说明,规定适用于组织在业务活动中形成和管理文件的能力;本文件则为 MSR 提供了实践指南。本文件所称“文件”<sup>1)</sup>等同于中文语境下的机关单位或组织的文件和档案。

本文件在符合 GB/T 34112 内容的同时为组织内实施 MSR 提供了实践指南。本文件包含建立和维护 MSR 的所有需考虑的因素。MSR 的实施通常以项目的形式执行。一个 MSR 能在如下情况实施:已经有文件系统或项目的组织想要评审和改进对这些系统或项目的管理,或是组织首次规划在文件生成和控制中运用体系化和可证实的方法。实施指南在上述情况下均适用。

组织决定实施 MSR 之前需要初步评估现有文件和文件系统已经识别重要改进过程中需要解决的风险和机遇。比如,在改变主要信息技术平台或外包一个高风险的业务过程时,采用 MSR 就相当于实施降低风险的策略。或者,MSR 能为重大改进提供一个标准化的管理框架,如将文件过程与特定业务过程集成处理或改进对于线上业务往来文件或使用社交媒体的业务的控制和管理。

根据组织的规模、性质以及复杂度,以及已经实施的 MSR 的成熟级别,本文件能灵活进行使用。每个组织所处的背景和复杂程度都是独特的,且组织的特定背景需考虑的因素还会对 MSR 实施产生影响。小型组织能对本文件中所描述的措施进行相应的简化,而大型或复杂的组织则可能需要一个多层次的管理体系,以有效实施和管理本文件中的各类活动。

本文件采用与 GB/T 34112 相同的结构,说明了为满足 GB/T 34112 内容而采取的措施,以及如何以文档记录这些措施。

- 第 4 章解决了如何分析 MSR 需求的问题。通过此分析,明确了 MSR 的范围,并定义了实施 MSR 与其他管理体系的关系。
- 第 5 章解释了如何从最高管理者处获取承诺。此承诺在文件方针、职责分配、MSR 的实施规划以及采纳文件管理目标中均能体现。
- 第 6 章解决问题,这些问题在高等级风险分析、组织所处背景分析(见第 4 章)以及可获得的资源(见第 7 章)表现。
- 第 7 章列出了 MSR 所需的支持,比如资源、能力、培训和沟通以及证明性文档。
- 第 8 章解决了对将要实施的文件过程的定义或评审以及规划的相关问题。包括组织的背景需求和范围(见第 4 章)、文件方针(见 5.2)、风险分析(见 6.1)以及为了满足文件管理目标(见 6.2)的实施过程中的资源需求。第 8 章解释了宜为 MSR 实施哪些文件过程和系统。
- 第 9 章和第 10 章解决了绩效评价以及改进 GB/T 34112 中的规划、目标和需考虑的因素的相关问题。

对于 GB/T 34112 中第 4~10 章中的每一条,本文件提供了以下内容:

- 满足 GB/T 34112 所需的必要活动——这些活动能按顺序实施,但其中一些活动需要以同样的背景分析并同步实施;
- 对措施的输入——说明了措施实施的起始点,且此输入可能是上一措施的输出;

1) 根据中国档案工作实际,“records”翻译成“文件”,等同于中文语境下的机关单位或组织的文件和档案(不包括档案馆藏档案),标题上采用“文件(档案)”,便于检索,也便于维护文件(档案)管理系列国际标准中“records”的本意,便于维护已经采标的国家标准使用的连贯性和更广泛推广应用。

——措施的输出——这些输出是实施措施后产生的结果,或者能在整个活动过程中传输。

本文件的使用对象是领导 MSR 实施和维护的负责人。本文件也可用于帮助最高管理者在其所在组织建立文件管理体系,定位其范围以及实施的决策,也可供负责领导 MSR 实施和维护的人员使用。关于如何设计可操作的文件过程的概念来源于 GB/T 26162—2021 中给出的原则。其他设计、实施、监控和改进文件过程、控制和系统时宜使用的原则性工具的国家标准和技术报告,能与本文件在实施更加细化的 MSR 业务要素中结合使用。

已经实施 GB/T 26162—2021 的组织能在体系化的和可证实的 MSR 方法指导下运用本文件来开发组织管理文件的基础设施。



# 信息与文献 文件(档案)管理体系 实施指南

## 1 范围

本文件描述了在设计和实施 MSR 时需要进行的各项活动,GB/T 34112—2017 中所规定的内容没有改动和减少。

本文件适用于不同规模的各类组织(例如:企业、政府机关、非营利组织等)。

所有需要实施 MSR 的组织遵循本文件。

注:本文件是依据 GB/T 34112—2017 内容制定的文件(档案)管理体系(MSR)实施指南,宜与 GB/T 34110—2017 和 GB/T 34112—2017 共同使用。

## 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 34110—2017 信息与文献 文件管理体系 基础与术语(ISO 30300:2011, IDT)

GB/T 34112—2017 信息与文献 文件管理体系 要求(ISO 30301:2011, IDT)

## 3 术语和定义

GB/T 34110—2017 界定的术语和定义适用于本文件。

## 4 组织背景

### 4.1 了解组织及其背景

组织背景宜决定和驱动 MSR 的实施和改进。本章旨在确保组织在实施一项 MSR 之前能够充分考虑其背景及需求。这些需考虑的因素通过对组织背景的分析予以满足。整个实施过程的第一步宜对组织背景进行如下各方面的分析:

- 识别内部和外部因素(见 4.1);
- 识别业务、法律及其他方面需考虑的因素(见 4.2);
- 界定 MSR 的范围(见 4.3)以及识别风险(见第 6 章)。

注 1:如果 MSR 的范围在初始阶段由最高管理者规定,在识别文件要素和需求之前,背景分析的范围也宜在其规定的范围内。

注 2:用于背景分析和明确需求的管理体系标准(MSS)方法与 GB/T 26162—2021 建议的分析过程(鉴定)兼容包含了文件规划要素(见第 6 章)和文件需求识别(见第 8 章)。

背景信息需遵循来源可靠性、准确性、及时性以及完整性。宜对信息的来源进行定期评审以确保背景信息的可靠性和准确性。

A.1 给出了关于组织内部和外部背景信息来源的案例以及潜在利益相关方案例。

在明确背景信息如何影响 MSR 的过程中,可能涉及的重要因素有:

- 竞争性市场如何影响高效过程的需求；
  - 外部利益相关方的价值观如何影响文件留存的决策或信息访问的决策；
  - 信息技术基础设施和信息架构如何影响文件管理体系或文件的可获得性；
  - 组织内部的技能和能力如何影响培训或外部援助的需求；
  - 法律法规、政策、标准和行业守则如何影响文件过程及其控制的设计；
  - 组织文化如何影响 MSR 需考虑的因素的合规；
  - 组织结构体系、业务和立法环境的复杂性如何影响文件方针、过程和控制(例如:跨法域管辖区)。
- 不同的组织,确定内部和外部因素还可能包含其他目标,比如包括其他的管理体系标准的实施。在上述情况下,并不一定要制定新的分析方法,对于上述分析进行调整就能满足需求了。

背景分析是一个连续的过程,它为 MSR 的建立和体系评价提供了依据(见第 9 章),并支持 MSR 的持续性改进(见第 10 章)。

输出:

GB/T 34112—2017 提出在分析过程中要有证明性凭证。例如:

- 内部和外部考虑因素清单；
- MSR 实施相关的手册或项目计划中的某一章；
- 一份关于组织内外部环境分析以及其与 MSR 的相互影响的正式报告；
- 一系列关于组织背景的文件。

#### 4.2 业务、法律及其他需考虑的因素

以 4.1 中的分析结果为出发点,评估与业务活动和所记录的文件相关的法律、业务和其他需考虑的因素。业务活动是用于明确影响文件产生和控制需考虑的因素的首要因素。

明确业务方面需考虑的要求宜考虑如下几个因素:

- 组织活动的性质(如:采矿业、金融咨询、公共服务、制造业、制药、私人服务、非营利组织、社区服务等)；
- 组织特定的形式或所有权(如:信托、企业或政府组织)；
- 组织所属的特定部门(即:公共部门、私营部门、非营利部门等)；
- 组织所属的司法管辖区。

业务需考虑的因素宜根据当前业务过程绩效以及未来发展计划进行明确。当组织正在实施自动化或电子化的业务过程时更需特别注意。因为在上述情况下组织的业务需考虑的因素有可能会变化,因此需要与新流程的发展及实施的负责人进行讨论。

为了明确所有适用于组织的强制性法律和监管手段,采取如下活动:

- 评审与行业相关法规的合规性需考虑的因素；
- 评审隐私和其他的文件数据管理法规的合规性。

A.2 给出了有关文件生成和控制的业务、法律和其他需考虑因素的案例,以及用以明确业务、法律及其他需考虑的因素。

输出:

为了遵循 GB/T 34112—2017,需强制地记录被识别出的业务、法律及其他需考虑的因素。既能全部记录在一起,也能按照不同的内容类型分别记录是十分必要的。证明性信息的类型如下:

- 按类型(如业务、立法)确定的需考虑的因素列表清单；
- MSR 实施相关的手册或项目计划中的某一章；
- 识别 MSR 需考虑的因素的正式报告书；
- 总结所有适用于组织(与文件产生和控制相关)的法律法规、强制规范或行业守则,生成一个列表清单；
- 判例文件(有关组织特定主要问题的一系列法律判例)。

### 4.3 界定 MSR 的范围

MSR 的范围由最高管理者来决定,这个决定明确了 MSR 的边界、包含条款、排除条款以及各个组成部分的角色及其相互关系。

此范围既能是综合考虑已经识别的要素(见 4.1)和需考虑的因素(见 4.2)之后得出的背景分析结果,也能在识别要素和需考虑的因素之前的初始阶段就由最高管理者制定。

范围包括如下方面:

- 识别组织包括哪些部分或功能。其范围能是整个组织,也能是一个区域或部门,或者是一个或一组具体的功能或业务过程。
- 识别其他相关组织的哪些部分或功能被包括以及它们之间的相互关系。
- 关于 MSR 如何与组织的总体管理体系及其他特定管理体系融合的说明(参考:ISO 9000 系列标准,ISO 24000 系列标准和 ISO/IEC 27000 系列标准)。
- 识别影响 MSR 的所有外包过程以及对于这些外包过程的责任实体的控制。

输出:

一份 MSR 需考虑因素的、限定 MSR 范围的证明性声明。此声明可单独列出,也可包含在其他 MSR 文档中,如文件方针(见 5.2)、MSR 实施手册或项目计划。

## 5 领导作用

### 5.1 管理承诺

明确最高管理者对于实施 MSR 的承诺,并且与组织实施的其他管理体系和资产(如:人力资源、财务和基础设施)同等详细。对于最高管理者管理承诺需考虑的因素,虽然不需要特定的活动来展示,但是它对于 MSR 的成功非常重要。管理承诺同样被包含在 GB/T 34112—2017 的其他与资源(见 7.1)、沟通(见 7.4)和管理评审(见 9.3)相关需考虑的因素中。

输出:

除了在文件方针(见 5.2)中,文件最高管理者对于 MSR 的管理承诺并非强制,只将其作为管理承诺的证据。承诺还能通过行动或声明证实,但是,由于组织的性质和复杂性,承诺的证据也宜在文件方针以外的文件上予以记录。包括但不限于如下内容:

- 董事会或管理委员会的会议记录;
- 策略和业务规划中的陈述/声明;
- 管理的决议和指示;
- 预算、业务案例;
- 沟通计划。

### 5.2 方针

由最高管理者定义的组织战略方向是文件方针的基础。文件方针由最高管理者制定,是实施和提升组织 MSR 以及提供 MSR 绩效评估基准的驱动因素。

最高管理者的指示需要在正式文档中声明。正式文档通常不由最高管理者起草,但是需要最高管理者正式批准,独立于撰写者。在不同组织中,最高管理者可能担任不同的职位,但是文件方针宜得到其中具有最高职位的领导的支持。

文件方针包含总体的指示、为实现目标如何生成和控制文件及实施原则。它能嵌入全局性的管理方针,用于多个管理体系标准的实施。在此场景下,文件方针不需要单独的管理支持。

文件方针需考虑的因素包括以下方面:

- 组织背景的分析和需考虑的因素识别(见 4.1 和 4.2);

- 组织目标及战略；
- 文件方针对其他组织方针的影响和关系；
- MSR 的范围(见 4.3)；
- 组织结构和授权。

文件方针是一个意向声明,包括如下内容(例):

- 宗旨；
- 关于文件产生和控制的高层级说明；
- 关于文件产生和控制的高层次责任和承诺；
- 关于方针将如何被实施的指示；
- 定义。

文件方针起草时宜充分考虑可读性,以能让所有使用 MSR 的用户都容易理解的形式起草。在文件过程和系统的实施中,一些包括决议的技术文件类文档被称为方针。当实施 GB/T 34112—2017 时,文件方针宜是独一无二且简短的文档,类似最高管理者的声明一样而且不包含对于目的、行动或文件过程的描述。

组织能运用 7.4 中的方法互相沟通文件方针。

输出:

在实施 MSR 时,被批准的文件方针是正式文档。组织宜确保文件方针在整个组织所有层级中得到传达和贯彻实施。文件方针是实施 MSR 的所有文件中的总领性文件。

## 5.3 组织的岗位、职责和权限

### 5.3.1 总则

合理规定和设置 MSR 的职责和权限,由于 MSR 涉及组织的各个层级,因此需要明确规定 MSR 设计、实施和维护方面的负责人。除了接下来各章中正式任命的管理代表和执行代表,为了实施 MSR,最高管理者宜为如下各项任务分配责任:

- 方针制定和批准；
- 资源分配；
- 程序和过程的制定和审批；
- 系统设计；
- 培训和指导；
- 方针、程序和过程的实施和维护；
- 合规的审核和监控；
- 绩效管理。

上述职责能被分配到组织的不同岗位上。能参照下述说明进行职责分配:

- 最高管理者负责授权和支持文件方针在整个组织中的应用；
- 在最高管理者中设置特定的岗位负责对 MSR 的领导；
- 业务部门的负责人需要确保所在部门的员工按照文件方针生成和管理文件；
- 文件专员负责文件过程和控制的设计、文件系统的实施和维护、负责员工在文件过程和控制以及文件系统使用上的培训,因为他们会影响到个体实践；
- 系统管理员负责确保文件系统功能是可靠的、安全的、合规的和全面的,同时要确保以体系化的方式管理文件(包括文件的迁移和变化)；
- 信息技术员工负责实施和维护持续可靠的管理文件所需的技术支持,有时包括系统的迁移；
- 全体员工都有责任按照文件方针在其活动中,通过使用组织的文件系统、过程和控制,生成和管理其活动的记录。

本章中需考虑的因素与 7.2 和 7.3 中需考虑的因素紧密相连,且宜同时实施。

**输出：**

职责分配是实施 MSR 过程所需的证明性文档中的一部分。职责分配能通过不同的形式进行记录,包括但不限于如下内容:

- 文件方针中高层次的职责(见 5.2);
- 管理代表和执行代表的任命文档;
- 工作描述或类似声明;
- 正式的责任授权声明;
- MSR 实施相关的手册或项目计划中的某 chapters。

**5.3.2 管理职责**

明确管理代表的岗位分配和责任界定。该岗位全面负责领导 MSR 的实施和维护。管理代表宜是组织最高管理者中的成员。基于组织的复杂性和即将实施的 MSR,领导作用宜与执行代表(如 5.3.3 所述)进行互补。最高管理者代表的职责宜包括以下几点:

- 需要时,批准关于计划、设计、维护和评价 MSR 和 MSR 项目的正式文档。
- 批准实施和维护 MSR 必需的资源分配。
- 批准实施和维护 MSR 相关的一到两个岗位的安排。岗位能分配到特定的部门,或者指定一个组织中复杂度和规模均合适的小组。
- 通过诸如沟通(见 7.4)和员工参与、授权、激励、表彰和奖励等方法,促进 MSR 行为兼容一致。
- 确定负责实施和维护 MSR 岗位上的个人(员工或承包商)所需的能力。

职责的范围、性质和文件均在 5.3.1 中列出。

**输出：**

- 如 5.3.1 所述。

**5.3.3 执行职责**

任命一个执行代表负责以下事项:设计和指导业务实施所需要的各类活动,并且在 MSR 上向最高管理者汇报。执行代表能由是一个组织内部员工或一个外部承包者所担任。

执行代表宜具备特定的文件职业素养和能力,具体需考虑的因素见 7.2。

执行代表的职责范围、性质和文档,见 5.3.1。

执行代表所承担的任务大体上以 GB/T 34112—2017 中的第 8 章和 GB/T 34112—2017 中的附录 A 所确定的内容为基础。

执行代表能协调一个或多个 MSR 小组的活动,以在执行层面实施和维护 MSR,并且负责绩效提升。

执行代表宜提供报告及支持性文档给最高管理者或特定管理代表(此处的管理代表负责 MSR 的实施和有效性,以及为业务过程的相关改进提供建议)。报告可根据组织需考虑的因素,在一定时间间隔或阶段进行递送。宜根据 GB/T 34112—2017 的附录 A 中的文件管理过程和控制进行管理。

与外部组织在 MSR 问题上进行交流联络同样是执行代表的职责。此处活动能包括但不限于以下内容:

- 向法律法规专家寻求建议;
- 遵循审核和质量控制专家需考虑的因素和指示;
- 指导产品或服务供应方(例如:软件供应商、业务实施顾问等)并与之协商;
- 从人力资源或信息技术承包商中获取额外的技能和协助。

管理代表和执行代表可由同一人员或同一团体担任,具体情况取决于组织的规模和复杂度,以及 MSR 的范围。

**输出：**

- 见 5.3.1。

## 6 规划

### 6.1 应对风险和机遇的措施

本章旨在对在保证 MSR 实现其预期结果过程中可能出现的战略风险进行规划。MSR 的成功实施需考虑的因素将对于上述风险进行的识别、分析和评估纳入 MSR 的实施规划中。因素分析(见 4.1)和需考虑的因素(见 4.2)宜与风险评估一起完成。本章应用于定义文件管理目标(见 6.2)以及明确实现目标所需的措施,这些措施被纳入 MSR 实施过程(见第 8 章)中。

建立 MSR 以协助组织管理不确定性对于其业务目标的影响。没有生成和留存充足的文件会增加企业的不确定性,并且对于实现组织目标的能力产生消极影响。建立 MSR 以协助对于不确定性及其影响的管理,是一种处理风险的方法。与 MSR 相关的战略机遇能被视为实现管理体系的积极因素或优势。这些优势与以下内容相关:提升组织的透明度和责任;改进业务过程;成本的效率和有效性;增进和加强组织与利益相关方、客户的关系。MSR 能帮助组织改进在实践中的劣势,并且帮助组织对抗外部业务环境改变所带来的风险。在决定把实施 MSR 纳入常规的风险管理框架之前,宜对上述风险和机遇进行识别、分析和评价。

在实施一个 MSR 时,在实现目标过程中的不确定事物均需被定义为风险。这样的风险评估还能帮助改进业务过程,并对业务目标产生积极影响。本章中各项需考虑的因素的宗旨是解决与 MSR 目标相关的风险和机遇的评估。这是 MSR 规划的一部分。组织能决定其使用哪种类型的风险管理方法,以及如何定义和实施用于减轻风险的措施。

此外,在文件本身和文件所属系统的相关方面,也会存在风险。这些风险属于操作风险,因此宜在实施规划(见 8.1)中进行评价。

根据风险和机遇的性质,需要制定不同类型和不同等级的应对方案。其中决定性的要素是:风险和机遇是否与 MSR 或业务目标在本质上有关。如果风险和机遇与 MSR 或业务目标需考虑的因素在 GB/T 34112—2017 的不同章中,即可视为单个活动进行处理。

若组织已经建立了一个正式的风险管理框架,其中的风险识别、分析和评价过程需要包括对于 MSR 的规划。

MSR 战略规划中需要考虑可能造成风险的各个不确定领域。这些领域可包括下述方面:

- 背景变化,例如:法律法规变更、经济和政策环境的变化以及组织结构变动等;
- 与生成和控制与支持组织完成任务和实现目标的各类证据相关的系统和过程;
- 实施和维护 MSR 的人力资源和技能;
- 预算和财务的影响和变化;
- 方针、目标和战略实现的测量和评价;
- 与其他已经实施的管理体系的关系。

战略风险和机遇的识别以及文件管理目标的规划能相互影响。因此,上述措施不是线性顺序。

通常,在此等级层面上对于风险的识别总体上宜与 MSR 相关,或者服务于一个特定的目标。

例如:与上文提到的“人力资源和技能”相关的风险,可与 MSR 本身相关,也可与文件管理的目标相关。

对于 MSR 本身,风险可以是管理者误解了管理体系的目标和其对于业务进程和目标的潜在影响,从而仅仅关注与 MSR 实施相关的认证过程。

例如:如果文件管理目标表述了一个特定系统(收集顾客相关过程中的电子文件)的需求,可能出现的风险就是员工拒绝改变和使用替换的技术(例如:运用电子邮件应用保留业务决策文件,以替代使用特定的系统保留文件)。

每个组织都有特定处理风险和机遇的措施。不同风险和机遇的应对措施也是特定的。这些措施宜被纳入实现目标和设计文件过程的措施中。

## 输出：

记录规划过程,并没有特定需考虑的因素。风险应对措施能被包含在实现目标的规划(见 6.2)中,或者作为规划中的组成部分单独列出。例如:

- 使用风险评估工具的任何输出(IEC 31010:2009 的附录 B 给出了此类工具的范围,ISO/TR 18128给出了一些例子);
- 实施处理风险和机遇相关措施的证明性文档。

## 6.2 文件管理的目标和规划

实施 MSR 或文件管理的目标,是根据组织所处背景、组织的需求和优先级所确定的。根据 MSR 的范围,确定实现这些目标的行动,并在整个组织内传达实现它们的目标和计划。

用于定义文件管理目标的输入包括:

- 对组织所处环境的分析和对组织需求的识别(见第 4 章);
- 文件方针(见 5.2);
- 风险分析和措施,以及识别处理风险的优先级(见 6.1);
- 对于现有文件过程的评审。

每个组织的文件管理目标都是特定的[可参考背景分析(见第 4 章)和风险分析(见 6.1)],与组织的战略和目标一致,并且能被评估。

在确定文件管理目标时,组织宜考虑现有被评估的文件和文件系统的充分性、被认为具有处理优先级的风险以及为使组织获取更多利润,需要改进的主要领域。

由于组织所处背景的变化(如:法规变更)、文件方针的变化、风险评估或绩效输出评价的变化,所以对文件管理目标在必要时进行更新或修改是十分必要的。宜运用 7.4 中所述的方法对文件管理目标进行讨论。

实现文件管理目标的措施同样需要被识别。每个目标可能需要通过一个或多个措施实现。措施需要根据以下需考虑的因素规划:

- 确定实施措施的预期输出。
- 明确何时、何地、如何以及何人承担并实施措施。
- 根据组织的需求、背景、规模和复杂程度,以及将要实施的措施的性质,能运用正式的项目管理方法,或者更为正式的有证明性文档的项目或行动规划来设计实现文件管理目标的措施。根据措施的规模和复杂度,上述方法可能会再产生一个或多个项目计划。

对于规划变更的控制,能通过正式的项目报告、计划和监控环节中的请求变更过程,或过程的重新设计来实现。

一个包含 MSR 实施的优先级和目标的业务案例,能够更加清晰和缜密地说明制定措施的过程。此案例包含以下内容:

- MSR 的范围(见 4.3);
- MSR 中需要处理的风险;
- 目标和规划;
- 实现目标的特定任务的优先级和时间节点;
- 给特定人员分配的职责;
- 项目基础;
- 额外人力资源和技能的需求;
- 其余资源的需求;
- 评估措施效果的方法。

这个规划的阶段,能够帮助组织理解 MSR 的相关性,并且明确一个组织中 MSR 项目所需的各类岗位和职责。

输出：

生成与文件管理目的相关的证明性信息是 MSR 需考虑的因素,但对于要生成的文档的形式并没有强制需考虑的因素。例如可包括以下信息：

- 特定文件目的的文档；
- 实施 MSR 所批准的证明性和承诺性文档；
- 业务案例或等价物；
- 带有关键里程碑的 MSR 项目规划。

## 7 支持

### 7.1 资源

对于 MSR 的实施和维护的规划(见第 6 章)包括评估所需资源的类型和数量,其次,获取管理层对于在需要时配置这些资源的承诺。

根据将要实施的措施范围,以及为了确保 MSR 的维护变成常规业务过程的一部分,资源分配能在不同的时期进行。资源可能是临时的或永久的,外部的或内部的。

MSR 设计、实施和维护所需的资源包括以下内容：

- 人力资源,合适的数量、级别和技能；
- 一个适用于组织文件管理过程和控制需求的信息与通信技术(ICT)环境；
- 财务资源；
- 设施和后勤,如:在需要时接收额外的员工。

对于为组织提供有关 MSR 设计、实施和维护服务的人员或组织,宜制定正式的安排。比如安排能包括以下内容：

- 职责说明；
- 特定能力需考虑的因素；
- 提供服务的可持续性；
- 在供应方合同即将结束时对工作的移交安排。

输出：

资源分配是最高管理者承诺的一部分,但是并没有对留存特定证明性信息的特定需考虑的因素。资源分配的典型文档,允许以 MSR 的预算、组织架构图、部门职责声明、系统、设备和 MSR 需考虑因素的其他基础设施的目录,以及合同书(如:外部提供的服务)等形式存在。

### 7.2 能力

需要确保在 MSR 中,员工有足够的能力胜任其分配的职责包括明确所需的能力、雇佣有相应能力的员工或承包人以及确保能力适用于岗位需考虑的因素。

根据组织的规模、复杂程度、岗位以及将要推行的措施,业务岗位所需要的能力会发生更改。

执行代表所需要具备的能力宜包含以下几点：

- 在信息管理领域的任职资格；
- 管理项目,包括项目的规划、监控和汇报等工作；
- 管理员工、承包人和团队；
- 为利益相关方的参与提供开发技术；
- 评价在特定领域的组织绩效,并且为组织的调整和改进提出建议。

对于设计和执行文件过程和控制的人员,具备的能力根据其岗位不同能分为不同的级别。但能力中比较典型的领域包括以下几个：

- 背景分析和需求分析；

- 为文件控制和维护制定程序、工具和方法；
- 制定并实施访问规则；
- 设计并使用系统以支持文件管理过程；
- 明确文件处置程序、规则并按其实施处置；
- 维护文件系统。

能力准则适用于所有代表组织的员工、承包人或临时员工。

在明确了实施 MSR、文件过程和系统所需的各种技能之后,能制定包含能力的职责或工作说明书。接下来,根据职责或工作说明书,评价当前员工的经验、资格和技能,能对现存差距进行评估并且实施相应的措施来满足能力需考虑的因素。通过上述过程,能:

- 培训和指导现有的员工；
- 再分配员工；
- 雇佣新的员工；
- 获得合同制员工。

用于获取必需能力的措施能通过以下方面进行评估:

- 根据基准进行个人绩效评估；
- MSR 绩效评价的结果(见第 9 章)。

**输出:**

GB/T 34112—2017 提出组织生成和留存说明不同岗位的员工能力的证据是十分必要的。包括描述人员技能、教育或培训的员工文件,以及对每个岗位上技能和能力的定义的输出是至关重要的。

### 7.3 意识和培训

需要运用一些策略来增强对 MSR 方针、目标和需考虑因素的意识,以及使员工了解其在实现与 MSR 一致性方面的岗位和责任。能通过不同的培训和意识培养项目,以及适用于现有项目的方法来实现。

培训和意识培养策略能包含以下内容:

- 员工的入门项目；
- 正式、系统的培训项目；
- 管理者和员工简报,例如,将其作为常规员工会议的一部分；
- 财务的或实物奖励；
- 在 MSR 特定领域和文件过程和控制的业务方面的补充培训；
- 7.4 中列出的沟通技巧。

为了适应组织的需求,培训能通过多种方式进行,包括以下方式:

- 面对面培训；
- 线上培训；
- 一对一培训,比如培训管理者时采用。

**输出:**

实施本章中需考虑的因素,并不必要有特定的证明性信息。对于培训项目的实施能通过多种方式呈现。下列内容是本章输出的内容,并且会根据组织的规模和复杂程度,以及培训和意识培养项目的主要有所变化:

- 项目设计概念；
- 教学计划；
- 管理计划；
- 项目评价计划；
- 项目内容；

- 培训材料,包括培训者的笔记和被培训者的材料;
- 项目评价;
- 出席记录。

## 7.4 沟通

沟通程序和方法的建立,是为了确保 MSR 的有效实施以满足 MSR 需考虑的因素。在制定此类程序和方法时,识别各类目标群体或受众非常重要。不同受众可需要不同的信息和沟通方法。关于 MSR 的沟通能嵌入现有的沟通策略中。

关于 MSR 的沟通程序宜包括:

- 沟通的范围和内容的总结;
- 沟通的方法;
- 沟通的职责;
- 评估沟通有效性的方法。

关于 MSR 的沟通内容宜包含以下内容:

- MSR 的目标;
- 实施 MSR 的好处;
- 岗位和职责;
- MSR 相关文档的地点和访问方式,包括实施要素;
- 与文件过程、控制和系统相关的运行程序;
- 对遵从文件方针、目标和运行元素的支持(如:文件系统的支持性服务)。

内部沟通方法的例子包括:

- 奖励措施,例如内联网公告、海报、竞赛和奖品;
- 宣传员,也就是宣传 MSR 信息的业务负责人;
- 常规业务部门会议的简报;
- 时事通信和公告板。

组织需要决定是否与外部利益相关方沟通 MSR、文件方针和目标。这需要对于以下几点有充分和明确的理解,包括谁是外部利益相关方、外部利益相关在组织中涉及利益的性质、外部利益相关方将会对 MSR 实施和可持续性产生的影响或潜在影响(见 4.1)。

例如,在以下两种情况时,沟通就非常重要:外部利益相关实体是组织供应链的一部分,可能使 MSR 中文件过程和控制的输出具有一致性和可持续性;如果有共享的业务过程,其他的实体能提出对组织文件系统的某些环节进行直接访问的需求。

根据与外部利益相关实体的关系、实体对 MSR 的影响或输入,组织能选择如何记录与其他实体在文件方针、目标和运行程序上的沟通。但是,如果外部实体与组织的日常业务过程相互作用,沟通宜包括各自的岗位、权力以及影响文件过程和控制文件系统使用的情形。

输出:

在实施 GB/T 34112—2017 时,组织有强制性的内部沟通上的证明性程序。如果组织决定在外部沟通 MSR,则还需要一个外部沟通程序,或一个同时包含内部或外部信息的通用沟通程序。

实施本项内容的额外输出包括:沟通的信息、结果或证据,以及在决定是否建立 MSR 时与外部利益相关方沟通的证明性决策文件。

## 7.5 证明性文档

### 7.5.1 总则

证明性文档建立和维护的目的,是描述 MSR 的核心要素以及他们之间的关系。文档中包括对描述 MSR 以及产生于 MSR 过程和控制的证明性文档的结构、格式、要素和控制系统的定义。

MSR 的规划、运行和控制的证明性文档,取决于组织的规模和 MSR 的范围。GB/T 34112—2017 制定了实施一个 MSR 所需的最少的证明性文档,但是如果需要,组织能生成额外的证明性文档用以确保对 MSR 的有效规划、运行和控制。

实施 GB/T 34112—2017 所需的证明性文档在每章中均有定义和解释。有一些特定的文档,如方针或程序被确定为是必须的。对其他证明性文档需考虑的因素而言,由于没有明确定义文档的特定类型,因此能通过不同的方式进行满足。

GB/T 34112—2017 的 7.5.1 可用于核对其他章中的证明性文档要求。表 1 给出了其他章中需要包含的证明性文档。

表 1 证明性文档需考虑的因素

证明性文档需考虑的因素	GB/T 34112—2017 章条号	指定文档
外部和内部要素	4.1	未指定
业务、法律和其他需考虑的因素	4.2	未指定
MSR 的范围	4.3	未指定
MSR 与其他管理体系的独立性和联系	4.3	未指定
文件方针	5.2	方针
岗位和职责	5.3	未指定
风险评估	6.1	未指定
文件管理目标和规划	6.2	未指定
能力需求	7.2	未指定
内部沟通	7.4	程序
外部沟通(有条件的)	7.4	程序
证明性文档控制	7.5.2	程序
文件过程设计	8.1	未指定
文件过程控制	8.1	未指定
绩效评价	9.1	未指定
内部审核	9.2	审核程序
不符合项和纠正措施	10.1	未指定
文件识别	A.1.1	未指定
对文件需考虑的因素	A.1.1, A.1.2, A.1.3, A.2.1	未指定
文件保存	A.1.1	程序; 处置时间表
文件获取方式	A.1.1	未指定
获取文件的节点	A.1.2.2	工作过程程序
技术的选择或变动	A.1.4	未指定
登记(有条件的)	A.2.1	程序
分类	A.2.1	分类方案
事件历史	A.2.1	程序
访问	A.2.2	访问规则

表 1 证明性文档需考虑的因素 (续)

证明性文档需考虑的因素	GB/T 34112—2017 章条号	指定文档
完整性、真实性、可用性	A.2.3	程序
处置	A.2.4	程序
移交和移除	A.2.4	程序
文件系统	A.2.5.1	文件系统的详细目录
在文件系统中实施决定	A.2.5.2	未指定
文件系统的可获得性和完整性	A.2.5.4, A.2.5.6	程序

### 7.5.2 证明性文档的控制

组织建立和维护控制 MSR 证明性文档的程序。程序宜包含不同级别的证明性文档、证明性文档的命名和编码的惯例、起草、评审和批准证明性文件的岗位和职责、允许作为证明性文档的格式和模板。

MSR 需考虑的因素的证明性文档(见 7.5.1),以及来源于文件过程和控制的设计、实施以及维护的证明性文档,使用 GB/T 34112—2017 的附录 A 中的文件过程和控制条款来进行管理。

除了文件控制,证明性文档的更新,需要有版本控制并宜遵守 7.4 中建立的沟通和分发程序。

ISO/TC 46/SC 11 的国际标准和技术报告,给出了设计和实施一系列文件过程和控制范围的指南的相关资源。

如果组织已经实施了其他管理体系标准(MSS),宜给出配套的证明性文档,且证明性文档程序宜适用于两个或多个 MSS。

输出:

——证明性文档程序的控制。

## 8 运行

### 8.1 运行规划和控制

组织确定、规划和实施实行文件操作过程和系统,以满足文件管理的目标(见 6.2),其中包含应对在 6.1 中已辨识的风险和机遇所需的措施。

大部分实施 MSR 的组织都会有现有文件、文件过程和文件系统,宜运用下文详细说明的 MSR 的程序进行评审,并且按照 GB/T 34112—2017 的附录 A 中所给出的文件过程和控制进行评估。对于现有文件、文件过程以及文件系统的评审,还有助于明确文件管理目标以及运行计划与控制。

宜对运行文件管理的过程和系统的需求进行明确和规划。组织通过以下方式来规划 MSR 的运行:明确将要运行的文件过程和系统、明确开展过程的准则、根据所开展过程的等级,给出与其等级相应的详细描述,包括与之相关的不同措施、输出、人员和系统。

在定义文件过程时,有必要确定需要哪种控制来证明每个过程都按规划实施。运营规划和控制的输入是对风险和机遇的分析,以及为应对这些风险和机遇而宜采取的措施(见 6.1)。

根据组织特定的需求所实施的生成和控制文件的运行过程,需要满足 GB/T 34112—2017 中附录 A 需考虑的因素。ISO/TC 46/SC 11 中与之相关的国际标准和技术报告可作为设计和实施这类过程的指南使用。本章中的内容宜与 8.2 和 8.3 中内容结合起来予以考虑。

对于任何外包的业务过程或文件过程,GB/T 34112—2017 都明确十分有必要对其进行控制。这类控制宜在与外包服务提供商签订的合同中详细说明并以证明性文档的形式记录下来。

与第 9 章相一致,由外包服务提供者所实施的过程宜与其他过程同等对待,接受同样的绩效评价。

## 输出：

本章中没有特定的输出。输出均被包含在 8.2 中。

## 8.2 文件过程的设计

文件过程和控制的设计包括对现有文件过程的评审或对新文件过程的设计。不论是评审还是新设计,均以针对组织工作过程的分析,以及为实现文件管理目标的设计为基础。对于文件过程和需要应用的技术的设计,会根据以下内容的不同范围和复杂度产生变化:组织所处背景分析、风险评估、业务过程需考虑的因素、组织的规模和性质(见 4.1 和 4.2)、业务措施的紧急程度。

帮助设计新的文件过程或改进原有文件过程的分析中宜包含 MSR 中确定的风险等级和机遇等级,对于文件过程的相关风险的评估和处理。

除了 GB/T 34112—2017 中的内容之外,组织宜依据 8.1 给出的以下规则设计文件过程:

- 以工作过程分析作为设计文件过程的基础。对工作过程进行分析有以下两个目的:明确文件需考虑的因素(见 GB/T 34112—2017 的附录 A)和理解如何实施文件生成和控制需考虑的因素(在附录 A 中详细列出)。GB/Z 32002—2015 为实施和分析工作过程提供了指南。
- 对于文件过程运行的风险的评估,以及这些风险会怎样影响组织业务过程中真实、可靠且可用的文件的生成。ISO/TR 18128 为评估与文件过程相关的风险提供了指南。

GB/T 34112—2017 中对于设计和实施文件过程需考虑的因素,见附录 A。GB/T 26162—2021 对文件过程的种类和实施过程中的核心概念给出了进一步的指南。

宜根据 GB/T 34112—2017 的附录 A 中的“控制”部分,来判断所设计的文件过程是否应用于业务过程。

虽然文件过程都遵从 GB/T 34112—2017 中附录 A 需考虑的因素,但是这并不意味着文件过程要以完全相同的方式运用到每一个组织中。

若文件过程与 GB/T 34112—2017 的附录 A 中的特定强制需考虑的因素相关,但是却不适用于一个组织时,并不强制执行所有的过程和遵守相关需考虑的因素。但是,做出这个决定的原因宜作为设计文件过程的一部分,以文件的形式予以证明。

若文件过程被外包,宜对其在以下方面进行控制:合同、服务等级协议、汇报和证明性文档需考虑的因素。

在按照 GB/T 34112—2017 的内容设计文件过程时,能考虑以下要素以判断是否成功地满足需考虑的因素:

下面 a)~d)是与文件的生成和捕获相关的要素;e)~h)是与控制过程(于 GB/T 34112—2017 的附录 A 列出)相关的要素。括号内的参考条目与 GB/T 34112—2017 的附录 A 相关。

注: ISO/TC 46/SC 11 中的国际标准和技术报告为实施文件过程和控制的评审和设计提供了指南。

- a) 组织确定每项业务过程应在何时、以何种方式生成并捕获哪些文件。

组织建立起一个体系化的过程,该过程用于分析每项业务过程生成和控制文件需考虑的因素。整个过程与 MSR 范围、文件管理目标和实施规划一致。这个分析能以组织决策的方式开展,但是其结果需要以文档形式记录。如何实施和记录这类分析可参照以下内容:

- 1) 标有文件生成点的业务过程流程图;
- 2) 每个业务过程的文件(文档)列表;
- 3) 对业务过程所产生的文件的广泛描述,按照程序为每个业务过程记录。

在上述分析中,组织还宜给出一个文件保留期限,期限记录在解释如何开展分析的特定程序中。保管处置期限分析程序确保充分考虑所有法律、业务和其余需考虑的因素,以及安排适当的人员保证决策的实施。分析的结果结合特定的业务过程在保管处置期限表中记录。

组织能运用不同的方法设计文件生成过程。GB/T 34112—2017 中的内容指出设计出的文件过程要确保文件由适当的人员或工具,在措施或交易将被文档记录时生成,并且用最适合的方法进行捕获。捕获文件的方法也是证明性信息的一部分。

- b) 组织确定了文件应包括的内容、背景和控制信息(元数据)(A.1.2)。

在捕获文件时,同时捕获其描述性和背景性的信息,能使文件被文件形成者以外的人们或者业务过程以外的人们识别和理解。GB/T 34112—2017 除了规定对负责文件的组织领域进行识别以外,没有规定捕获哪些信息。但是为每个工作过程,以文件形式记录描述性信息的捕获要点是十分必要的。这些信息能包含在对每个业务过程的分析输出中(A.1.1)。

根据业务部门、规模和组织的复杂程度,可在元数据架构中预定义宜捕获的信息。ISO 23081-2 为文件元数据方案提供了指南。

制定出的元数据方案必然包括 GB/T 34112—2017 的 A.2.1 中的控制信息。

- c) 组织决定文件应以何种格式或结构生成和捕获(A.1.3)。

对要生成的文件的识别(A.1.1)包括文件的格式和结构。每个业务过程都宜以文件形式记录上述内容。

- d) 组织宜确定生成和捕获文件的适用技术(A.1.4)。

对要生成的文件的识别(A.1.1)包括有关运用哪些技术生成和捕获文件的决定。每个业务过程都宜以文件形式记录上述内容。在功能单一且员工较少的小型组织中,上述内容能通过记录生成文件的决定(运用纸质方式还是计算机系统的方式)和对计算机应用的选择。

- e) 组织明确在文件过程中应生成哪些控制信息(即:元数据),以及这些控制信息如何能够与文件及其日后的管理联系起来(A.2.1)。

设计一个在任何被需要时都能控制和管理文件的文件过程,需要根据文件相关的工作过程对其进行分组。组织能运用一个分类方案(正式的、文档记录的分组计划)来完成分组。任何业务过程上的变更都能在分类方案中反映出来。

在必要时,需设计一个正式的对于每个文件进行唯一识别的过程,以及与之相关的文件记录程序。

在这些文件过程中产生的信息可作为文件的控制信息(元数据)。组织决定如何管理这些控制信息,例如,使用元数据方案。

在小型组织内,这种需考虑因素能通过以下方式满足:根据组织广泛的业务活动,这些活动可能存在于组织选用的计算机应用中,或以纸质文件为基础的存储系统中,记录生成和保存不断积累的文件的决定,记录针对组织员工的相关说明。

- f) 组织宜为文件的长期使用建立规则和使用场景(A.2.2)。

明确访问文件的过程,需要分析文件的使用和识别相应的访问方式或使用许可。获访问规则的制定和记录,要包括所有的强制规定。

规则实施后,能定义能够查看或使用文件的人员和他们的许可,以及在保存文件的系统中实施这些规则。

- g) 组织宜明确如何维护文件的持续可用性(A.2.3)。

对于电子文件而言,文件在日后的可用性非常重要。设计和实施这个过程(对于任何形式的文件)宜考虑到各类安全问题,比如未经授权的使用、篡改、移除、隐藏及破坏。对于实施 GB/T 22080 的组织而言,上述安全需求已经被包含在内。

GB/T 34112—2017 表达了保存过程需考虑的因素。这些需考虑的因素包括使用相关的媒体或技术的标准,以及一个维护可用性的周期性检查的程序。如果在安全性约束中使用了加密,对此约束的界限以及解密文件的方法进行确定和记录。

- h) 组织实施经过批准的文件处置(A.2.4)。

根据 GB/T 34112—2017 设计文件处置过程,包括以下内容:建立程序管理对文件以及有关文件保存期限的附件的处置、授权文件处置决定、实施文件处置决定以及对文件的处置包括在需要时移交给另一个组织、迁移或改变存储地点以及销毁文件。

输出：

- 文件过程的设计；
- 文件过程嵌入业务过程的程序；
- 文件控制工具和支持性的背景分析,如:程序、分类体系、元数据方案、访问规则、安全性模型、处置方针或真实性；
- 系统需考虑的因素和技术说明书；
- 技术选择和获取的证明性文档；
- 系统设计和配置的证明性文档；
- 对过程、程序和系统的评审；
- 培训材料。

### 8.3 文件系统的实施

实施文件系统需考虑的因素在 GB/T 34112—2017 的 8.3 中进行了规定,GB/T 34112—2017 的 A.2.5 作为补充。两者都宜作为一个整体进行全面理解。

满足 GB/T 34112—2017 内容的文件系统能有多种格式,例如：

- 留存和管理事务文件的业务应用或系统；
- 按照需求再次生成文件的数据库；
- 用于自动捕获和管理文件的专业软件。

这些系统能由组织自主管理,也能由外部服务提供商管理。在这两种情况下,责任方都宜自始至终有能力捕获、管理文件并提供访问文件的渠道。除此之外,还宜在所有种类的系统变更中,有能力以保持可获取、可靠、可信和可访问的方式输出文件或文件元数据。

GB/T 26162—2021 建立了通用的文件系统的特征,以及实施文件系统的核心概念。GB/T 34840.1—2017、GB/T 34840.2—2017 和 GB/T 34840.3—2017 给出了电子办公环境下的文件原则和功能要求,并且能用于确定内容和选择适用的软件。在设计保存文件系统的实施和维护时,宜运用 ISO/TC 46/SC 11 开发的其他国际标准和技术报告。

一个组织能运用多个文件系统保存文件,但是需要明确全部保存文件的系统以及他们的责任方。

基于文件需求和文件管理目标,对于文件系统绩效的周期性的监控,宜确保以下几点：

- 文件系统能提供业务领域开展工作所需的功能；
- 文件系统按照其设计说明书运行；
- 文件系统能够保证需要使用的人员在需要时可获得；
- 文件系统宜以一个持续的可靠的基础上运行,预案能在系统发生变故或基础设施故障时被触发；
- 文件系统宜包括业务连续性和容灾机制(灾难复原)。

管理文件系统的运行意味着确保文件系统不仅要能以可靠、安全和兼容为基础持续运行,还要覆盖组织的全部业务活动。上述需考虑的因素能通过以下内容实现：

- 系统管理和维护运行的文件记录和实施程序；
- 按照设计说明书对于系统进行的周期性检测；
- 在系统失效、用户出现问题或投诉时,分析并实施纠正措施；
- 评估组织的员工运用其他(没有文件的)系统的等级和原因；
- 对于系统可访问性和可用性的周期性检测；
- 监测系统安全；
- 在任何业务需求、利益相关方期望或法律法规要求出现变更时,对系统进行评估,并且在必要时对系统进行更改以满足上述需求的变化；
- 实施必要的措施,以确保能够对所有组织的新功能或业务过程的文件进行管理。

输出：

- 强制的证明性信息包括以下内容：
- 管理文件的系统清单；
  - 系统实施和更改的证明性文档；
  - 维护系统的程序；
  - 访问系统的规则；
  - 为系统测试提供证据的证明性文档。

只要组织实施了信息安全项目,不论此项目是否以 GB/T 22080 为基础,同样的安全管理需考虑的因素(包括上述记录文件信息)适用于这些保存文件的系统。

## 9 绩效评价

### 9.1 监控、测量、分析和评价

#### 9.1.1 确定如何监控、测量、分析和评估,及其内容

组织测评 MSR 的有效性,监控文件过程、控制和系统,以完成以下目标:提供支持持续改进的信息,或者指出纠正措施的需求(见 10.1)。

为了明确哪些内容需要测量和监控,组织宜考虑以下因素:

- 评定由组织特定领域的文件或文件系统的不足导致的业务风险的等级；
- 其他管理体系标准的应用；
- 利益相关方需考虑的因素(见附录 A)；
- 法律法规的要求；
- 近期的新过程、控制或系统在业务领域如何实施。

为了应对任何组织背景环境中的变更(见第 4 章),监控和测量的准则宜定期进行评审和修改。

根据被评估的内容,对文件过程、控制和系统进行监控、测量、分析和评价的方法也会发生变化。这些方法能是定量的或定性的,能包括如下方法:

- 用户调查；
- 问题清单；
- 观察报告；
- 系统使用情况统计数据的收集和分析；
- 系统操作数据的分析,如:故障停机时间、死机状态、数据丢失等。

根据被评估的内容,监控和测量的频率同样会发生变化,例如:

- 一个大型组织在日常评估特定的业务功能；
- 一个小型组织以每年为周期评估整个组织；
- 由于不能满足法律法规需考虑的因素的风险评估的结果,组织需在更规范的基础上评估其 MSR；
- 在 MSR 实施中特定阶段完成时进行评估。

输出：

虽然证明性文档并不是本章需考虑的因素,但是在实施过程中产生和获取的结果可参照以下内容:

- 监控和测量的准则；
- 监控、测量、分析和评价的方法；
- 监控和测量的工具,如:提问清单和问卷；
- 监控和测量的输出,如:统计数据、访谈记录、观察记录、系统报告、测试结果、调查；
- 监控和测量的时间安排。

### 9.1.2 对于文件过程和文件系统运行绩效,以及 MSR 有效性的评估

评价监控和测量的结果,是为了确保组织的 MSR 过程中措施的整合和行动实施的有效性(见8.1)。组织确保 MSR 的绩效满足业务需求、法律法规需考虑的因素并且提升客户和利益相关方的满意度。在做出每个评估之后,都宜对监控和测量的结果进行分析和评价。然而,对于那些需要运用累计结果的分析,如趋势分析或对于管理报告宗旨的分析而言,能根据业务需求进行分析,如每季度一次、每年一次。分析和评价的输入信息来源于监控和测量的结果(见 9.1.1)、内部体系审核(见 9.2)、管理评审(见 9.3)以及任何周期性的或项目基础类的报告所明确有必要性的内容。组织应用上述数据来测量 MSR 的适用性和有效程度,以及评价哪些地方能进行改进。

组织宜建立、实施并维护对于 MSR 有效性的绩效评价,包括文件过程、控制和系统的绩效评价。对文件过程或文件系统的监控和评价是 GB/T 26162—2021 中所列出的基本原则的一部分。如果一个组织实施 GB/T 26162—2021,其监控和评价程序也能符合和遵循 GB/T 34112—2017 的内容。

为了确保 MSR 按照文件方针和需考虑的因素以及用户满意度操作,绩效评价宜周期性地进行。

如果发现绩效评价结果不足,宜对 MSR 以及文件过程和控制进行修正。必要时,宜在不符合项产生以前采取措施以处理反向的趋势或结果。见 10.1。

输出:

——评价报告。

### 9.1.3 评估有效性

对 MSR 进行监控和测量的目的是,评估 MSR 在满足文件方针需考虑的因素、实现文件管理目标以及满足业务需求和利益相关方期望上的有效性。

评估 MSR 有效性的输入信息包括绩效评价的结果(见 9.1.2)、内部体系审核(见 9.2)和管理评审(见 9.3)。

MSR 的有效性能通过以下要素判定,如:

- 一个符合组织宗旨的现行文件方针(见 5.2);
- 能够满足当前和未来短期的业务需求并且可行的现行文件管理目标(见 6.2);
- 根据业务、法律和其他需考虑的因素的变动,而修改的文件方针、目标、文件过程和控制(见 4.2);
- 在合理程度上,为维护 MSR 分配资源(见 7.1);
- 与组织的规模和性质以及 MSR 的范围相应,对于岗位、职责和权力进行充分的定义(见 5.3),并且为每个岗位安排合适的有能力的人员(见 7.2);
- 对实施、汇报和推行 MSR 意识的负责人的绩效评估(见 7.2);
- 文件过程和系统的绩效输出(见 9.1.2);
- 存在业务过程中运用 MSR 和实施文件过程的全套证明性文档(见 7.5);
- 实现组织战略、管理和财务目标的文件管理体系(见 8.3);
- 一个有关 MSR 的培训和意识的规划以及沟通策略,此规划和策略均为现行的,被周期性实施并且按照文件方针、目标、文件管理过程和控制(见 7.3 和 7.4)的变化进行修订;
- 评估用户和利益相关方满意度的结果(见 9.1.2)。

输出:

绩效评价的数据和证明性文档宜作为绩效评价过程的证据被保留下来。例如:

- 评估 MSR 有效性的证据;
- 绩效评价安排和计划;
- 绩效评价程序;
- 绩效评价的准则和要素;

- 绩效评价的结果；
- 差距评估,包含一个措施列表；
- 持续的监控数据；
- 监控报告。

## 9.2 内部体系审计

组织确定内部体系审核的频率并以其评估 MSR 是否与需求一致、是否根据文件方针和目标的变化得到有效的实施和维护。见 GB/T 19011 中提供的有关内部审核、审核员的特征、审核计划和安排以及审核报告的指南。

内部体系审核宜由不参与 MSR 实施的人员负责。一个审核程序在设计时宜满足 GB/T 34112—2017 的内容。在实施不同的 MSS 时,组织能实施多体系的内部审核。

为了确定 MSR 是否有效的实施和维护,评估以下内容:

- MSR 相关证明性文档的充足性,和实际上文档的反映程度；
- 文件方针和目标的流通实施情况；
- 评审组织所处环境并根据变化做出调整的频率；
- 人员对于被分配的岗位和职责的理解；
- 为了维护 MSR 所提供的支持是否充足；
- 文件过程和控制的实施和保持是否与其设计相一致。

输出:

- 审核规划；
- 内部审核报告和支撑性证明性文档；
- 一些组织能发现内部审核的记录程序非常有用,尤其在组织整合不同管理体系时。

## 9.3 管理评审

最高管理者执行 MSR 的评审工作,来确定当前 MSR 的绩效并确保 MSR 持续的适用性、充分性和有效性,此外还根据需要指导改进和变化。管理评审是对于 MSR 的全面评估,而不是仅仅关注其中一个特定的领域。但是,对于已经被确定的有风险的领域,能给予特别关注。

管理评审的输入信息包括:

- 之前管理评审的输出；
- 组织所处的环境背景(见第 4 章)；
- 监控、测量、分析和评价的结果(见 9.1)；
- 之前的内部体系审核(见 9.2)。

管理评审的频率取决于组织的需求和所处的环境背景。影响因素有:

- MSR 是新的还是已经被使用了一段时间；
- 之前管理评审的输出和响应；
- 之前审核的结果；
- 利益相关方的期望；
- 新的或在适用的法律法规上的变化。

实施 MSR 的管理复审能通过评审以下方面执行:

- 之前所实施的管理评审和措施；
- 任何可能影响 MSR 范围或组织风险等级的内外部变化；
- 之前监控和测量的结果；
- 之前内部体系审核的结果；
- 在监控、测量和审核中实施的纠正措施；

——能证明持续改进的机遇和措施的证明性文档。

为了评审 MSR 并且把握其持续改进的机会,管理者宜考虑:

- 持续调整 MSR,使之与组织影响 MSR 的战略方针相一致;
- 确保 MSR 的范围能够覆盖组织业务过程;
- 影响 MSR 的组织环境背景变化,比如法律法规变更、利益相关方的投入,或由于组织结构变化而产生的组织功能的变动;
- 复审文件方针和(或)目标的需求;
- 持续维护和改进 MSR 提供的资源和技能的充足性;
- 组织的员工和承包者对于 MSR 的认识和理解程度,以及对他们遵守文件方针和目标需考虑的因素;
- MSR 是否已经或将会继续实现其预期输出。

输出:

GB/T 34112—2017 提出有管理评审的证明性信息是十分有必要的。

评审的产物包括管理者的决定、与改进 MSR 过程或者改进 MSR 整体有效性相关的措施,以及对 MSR 的改动等的证明性文档。MSR 的改动能影响文件方针、目标或资源。

## 10 改进

### 10.1 不符合项控制和纠正措施

组织宜做到识别与 MSR 需考虑的因素不一致的不符合项、采取并实施适当的措施、评估造成不符合项的原因以及在必要时采取措施以消除上述原因。

可能造成不符合项的情况如下:

- 监控和测量(见 9.1);
- 内部审核(见 9.2);
- 管理评审(见 9.3);
- 点对点模式(ad hoc)报告。

需要对产生不符合项的原因进行分析。在需要的时候,还需要实施纠正措施。控制、容纳或纠正不符合项根据如下内容进行:

- 风险等级;
- 不符合项影响的程度;
- 实施必要措施所需资源的可获取度。

实施纠正措施的规划能包含以下内容:

- 分配岗位和职责;
- 确定需要实施的特定措施;
- 如果需要,分配额外的资源;
- 制定工作计划并且规定成果和输出;
- 在措施实施过程中进行汇报。

在评估实施措施需求或者实施措施程度,以消除造成不符合项的原因时,宜考虑以下因素:

- 对于组织而言,风险的等级;
- 对于 MSR 而言,风险的等级;
- 对于文件过程、控制和系统上的适当运行而言,风险的等级;
- 造成风险的原因复发的可能性;
- 纠正措施实施时需要的资源。

根据 5.3 中所识别的指定组织员工和承包者的职责,相关人员宜负责完成纠正措施的评审工作。

由此,这类报告给以后进行定期的监控和测量、内部体系审核和管理评审提供着手点,然后成为持续改进过程的一部分。

输出:

GB/T 34112—2017 提出留存产生于实施控制和纠正不符合项措施过程的证明性信息是十分必要的。可参照以下内容:

- 不符合项的证明性文档;
- 对于要实施的纠正措施的描述;
- 若能,决定不实施纠正措施的证明性文档;
- 实施纠正措施规划的证明性文档;
- 实施纠正措施的证据;
- 纠正措施的评审;
- 消除不符合项产生原因的纠正措施的需求评价;
- 预防措施规划的证明性文档;
- 实施预防措施的证据;
- 预防措施的评审。

## 10.2 持续改进

组织通过维护由高层管理者领导的规划、支持、业务和绩效评价这个循环过程,能提高 MSR 的有效性。同时,还能提高组织的以下能力:管理其文件长期可用的能力、满足其责任的能力、支持其业务需求的能力。组织需要证明持续改进循环过程正在运行,以确保组织文件方针和目标适宜,即与组织宗旨和其战略方针相一致,并且能够通过更新升级的文件过程、控制和系统反映出来。

持续改进循环过程的证实能通过以下内容表现出来:

- 持续的绩效评价结果;
- 实施纠正措施;
- 实施改进措施;
- 修订文件方针和目标;
- 根据变更需要修订 MSR 的支撑设施;
- 持续性的组织场景化和风险分析。

输出:

- 持续改进循环过程的输出上述指标的证明性文档。

**附录 A**  
(资料性)  
关于信息来源和支持组织背景分析需考虑因素的示例

#### A.1 信息来源

关于组织外部背景的信息来源包括：

- 来自或关于利益相关方的信息；
- 法律、法规、标准、行为守则、行业监管规则、公司治理规则和指示；
- 组织的诉讼文件和影响组织的监管措施；
- 政府或行业分析师所给出的经济、财务或环境分析；
- 媒体报道。

组织内部背景的信息来源包括：

- 组织的核心文档,如方针、战略、业务规划、年度报告等；
- 审核报告；
- 组织的结构、岗位、职责和授权的定义；
- 内部标准、指南和行为守则；
- 业务过程图或描述；
- 技能评估；
- 信息系统详细目录清单；
- 信息或数据模型；
- 利益相关方分析；
- 风险评估；
- 信息安全框架；
- 实施其他管理体系标准的背景分析；
- 项目管理方法论；
- 采购和承包模型；
- 对组织文化的理解(此部分能不用文档记录)。

利益相关方包括：

- 代表组织工作的内部员工和承包者；
- 在管理文件中起领导作用的内部员工,如审核、风险、法律、承诺、信息技术；
- 业务合作伙伴,如研究合作者、贸易合作伙伴；
- 股东、业主、受托人、董事；
- 产品和服务供应商；
- 客户；
- 对组织及组织所从事事务感兴趣的市民、非政府组织和其他社群团体；
- 可能对组织进行监督或监管的实体；
- 政府,包括组织运行所在的跨不同司法管辖区的多个政府。

#### A.2 需考虑的因素

有关文件生成和控制的业务需考虑的因素包括但不限于如下内容：

- 需考虑在执行或完成特定业务过程时,生成文件(包括但不限于基于网络的事务,以及新兴技术例如社交媒体,移动计算和云计算中的事务)；

- 需考虑在财务/运营报告和控制过程中,生成文件;
- 需考虑内部和外部报告时生成文件;
- 需考虑控制和监控外包服务或业务时生成文件;
- 需考虑分析和规划时生成文件;
- 需考虑对不同地点和超过特定时间段的文件,进行访问控制;
- 需考虑在访问和使用文件时需要提供证据(如:私人数据);
- 需考虑对文件中包含的信息进行共享和再利用。

与文件生成和控制相关的法律内容包括但不限于如下内容:

- 生成特定文件需考虑的因素;
- 为特定的利益相关方,如股东或客户,提供与组织活动相关信息需考虑的因素;
- 文件留存需考虑的因素(如给与特定的时间或项目有关的文件设置相应的文件保管期限);
- 以特定格式保存文件需考虑的因素;
- 在特定地点保存文件需考虑的因素;
- 对文件提供访问需考虑的因素和访问方式规定;
- 向其他组织或管辖方移交文件需考虑的因素。

其他与文件生成和控制相关需考虑的因素包括但不限于如下内容:

- 实践过程中自发遵守行为守则需考虑的因素,包括对于其他管理体系标准的实施;
- 为满足外部利益相关者期望,让相关者能够获取的特定文件。

在识别业务、法律和其他需考虑的因素时,可通过一部分内部和利益相关方获取援助,例如:

- 精通民法和不成文法的法律专家,以及组织与这些专家的交流(这对组织在不同的司法管辖区中运行非常重要);
- 对于其业务领域有深刻理解的员工;
- 文件、信息技术和系统专员;
- 审核员、风险和其他合规性专员;
- 对组织中实施 MSR 的过程有兴趣的文件/档案机构或控制实体。

## 参 考 文 献

- [1] GB/T 19011 管理体系审核指南(GB/T 19011—2021,ISO 19011:2018, IDT)
  - [2] GB/T 22080 信息技术 安全技术 信息安全管理 体系 要求(GB/T 22080—2016,ISO/IEC 27001:2013, IDT)
  - [3] GB/T 26162—2021 信息与文献 文件(档案)管理 概念与原则(ISO 15489-1:2016, IDT)
  - [4] GB/T 26163.1—2010 信息与文献 文件管理过程 文件元数据 第1部分:原则(ISO 23081-1:2006, IDT)
  - [5] GB/Z 32002—2015 信息与文献 文件管理工作过程分析(ISO/TR 26122:2008, IDT)
  - [6] GB/T 34840.1—2017 信息与文献 电子办公环境中文件管理原则与功能要求 第1部分:概述和原则(ISO 16175-1:2010, MOD)
  - [7] GB/T 34840.2—2017 信息与文献 电子办公环境中文件管理原则与功能要求 第2部分:数字文件管理系统指南与功能要求(ISO 16175-2:2011, MOD)
  - [8] GB/T 34840.3—2017 信息与文献 电子办公环境中文件管理原则与功能要求 第3部分:业务系统中文件管理指南与功能要求(ISO 16175-3:2010, MOD)
  - [9] ISO 9000 Quality management systems—Fundamentals and vocabulary
  - [10] ISO 13008 Information and documentation—Digital records conversion and migration process
  - [11] ISO/TR 13028 Information and documentation—Implementation guidelines for digitization of records
  - [12] ISO 14001 Environmental management systems—Requirements with guidance for use
  - [13] ISO/TR 15489-2 Information and documentation—Records management—Part 2: Guidelines
  - [14] ISO/TR 18128 Information and documentation—Risk assessment for records processes and systems
  - [15] ISO 23081-2 Information and documentation—Managing metadata for records—Part 2: Conceptual and implementation issues
  - [16] ISO/IEC 27000 Information technology—Security techniques—Information security management systems—Overview and vocabulary
  - [17] ISO 28000 Specification for security management systems for the supply chain
  - [18] IEC 31010: 2019 Risk management—Risk assessment techniques
-