ICS 35.040
L 80

中华人民共和国国家标准

GB/T 28450—2020/ISO/IEC 27007:2017
代替 GB/T 28450—2012

信息技术　安全技术
信息安全管理体系审核指南

Information technology—Security techniques—Guidelines for information security management systems auditing

(ISO/IEC 27007:2017,IDT)

2020-12-14 发布　　2021-07-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 28450—2012《信息安全技术　信息安全管理体系审核指南》，与 GB/T 28450—2012 相比，主要技术性变化如下：

——删除了 ISMS 特定审核原则的内容（见 2012 年版的 4.2）；

——删除了审核方案管理流程图（见 2012 年版的 5.1）；

——删除了审核方案内容（见 2012 年版的 5.2.2）；

——增加了审核方案管理人员能力的内容（见 5.3.2）；

——增加了审核方案范围和详略程度确定的内容（见 5.3.3）；

——增加了审核方案风险识别和评估的内容（见 5.3.4）；

——修改了审核方案实施的内容（见 5.4，2012 年版的 5.4）；

——删除了审核方案记录的内容（见 2012 年版的 5.5）；

——删除了审核组长指定的内容（见 2012 年版的 6.2.1）；

——删除了实用帮助——信息收集注意事项（见 2012 年版的 6.5.4.1）；

——删除了审核报告批准的内容（见 2012 年版的 6.6.2）；

——删除了能力概念图（见 2012 年版的 7.1.1）；

——删除了个人素质的内容（见 2012 年版的 7.2）；

——增加了个人行为的内容（见 7.2.2）；

——删除了 ISMS 特定及相关专业知识和技能的内容（见 2012 年版的 7.3.3）；

——增加了管理体系审核员特定领域与专业知识和技能的内容（见 7.2.3.3）；

——增加了多领域管理体系审核知识和技能的内容（见 7.2.3.5）；

——删除了教育、工作经历、审核员培训和审核经历的内容（见 2012 年版的 7.4）；

——增加了审核员能力获得的内容（见 7.2.4）；

——修改了审核员评价的内容（见 7.3、7.4、7.5，2012 年版的 7.6）；

——重新组织了附录的内容，删除了原标准的五个附录，增加了附录 A：ISMS 审核实践指南，与 ISO/IEC 27007:2017 附录 A 保持一致。

本标准使用翻译法等同采用 ISO/IEC 27007:2017《信息技术 安全技术 信息安全管理体系审核指南》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 19011—2013　管理体系审核指南（ISO 19011:2011，IDT）

——GB/T 22080—2016　信息技术　安全技术　信息安全管理体系　要求（ISO/IEC 27001:2013，IDT）

——GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇（ISO/IEC 27000:2016，IDT）

本标准做了下列编辑性修改：

——在引言中对本标准中涉及的部分术语和定义，与其他标准相关内容的关系进行了说明；

——在参考文献中增加了国际文件 ISO/IEC 27017。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准起草单位:北京时代新威信息技术有限公司、中国网络安全审查技术与认证中心、中国电子技术标准化研究院、全国组织机构统一社会信用代码数据服务中心。

本标准主要起草人:王新杰、王连强、张剑、上官晓丽、孙镇、赵捷、郑玮、陈剑博、郭乐宇、汪洋、曹宇、程瑜琦、王姣、孙泰、李晟飞。

本标准所代替标准的历次版本发布情况为:

——GB/T 28450—2012。

引　言

本标准提供了下列指南：

——信息安全管理体系(ISMS)审核方案的管理；

——遵循 GB/T 22080—2016 实施内部和外部审核；

——ISMS 审核员的能力和评价。

本标准宜与 GB/T 19011—2013 中包含的指南一起使用。

本标准遵循 GB/T 19011—2013 的结构，ISMS 审核所需的 ISMS 特定指南，用字母“IS”进行标识。

开展 ISMS 审核时，本标准新增的 ISMS 特定指南宜与 GB/T 19011—2013 配合使用，用字母“IS”进行标识”。

GB/T 19011—2013 提供了关于审核方案管理、管理体系内部或外部审核实施以及管理体系审核员能力和评价的指南。

本标准未声明组织规模要求，可适用于所有用户，包括中小型组织。

本标准中涉及的部分术语和定义，与其他标准相关内容的关系说明如下；

——国际标准中的“Procedure”，在 GB/T 19011—2013 中翻译为“程序”，而在 GB/T 22080—2016 中翻译为“规程”，因本标准同时引用了这两个标准的原文，故本标准中出现该术语的地方均采用其原标准中的定义；

——国际标准中的“Implement”，在 GB/T 19011—2013 中翻译为“实施”，而在 GB/T 22080—2016 中翻译为“实现”，因本标准同时引用了这两个标准的原文，故本标准中出现该术语的地方均采用其原标准中的定义；

——国际标准中的“Maintain”，在 GB/T 19011—2013 中翻译为“保持”，而在 GB/T 22080—2016 中翻译为“维护”，因本标准同时引用了这两个标准的原文，故本标准中出现该术语的地方均采用其原标准中的定义；

——国际标准中的“Documented information”，在 GB/T 29246—2017 中翻译为“文档化信息”，而在 GB/T 22080—2016 中翻译为“文件化信息”，因本标准引用了 GB/T 22080—2016 的原文，故本标准中出现该术语的地方均采用 GB/T 22080—2016 中的定义；

——国际标准中的“Context”，在 GB/T 29246—2017 中翻译为“语境”，而在 GB/T 22080—2016 中翻译为“环境”，因本标准引用了 GB/T 22080—2016 的原文，故本标准中出现该术语的地方均采用 GB/T 22080—2016 中的定义；

——国际标准中的“Continuity”，在 GB/T 29246—2017 中翻译为“持续性”，而在 GB/T 22080—2016 中翻译为“连续性”，因本标准引用了 GB/T 22080—2016 的原文，故本标准中出现该术语的地方均采用 GB/T 22080—2016 中的定义。

信息技术　安全技术
信息安全管理体系审核指南

1　范围

本标准在GB/T 19011—2013的基础上，为信息安全管理体系(以下简称ISMS)审核方案管理和审核实施提供了指南，并对ISMS审核员能力提供了评价指南。

本标准适用于需要理解或实施ISMS的内部或外部审核，或需要管理ISMS审核方案的所有组织。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 19011—2013　管理体系审核指南(ISO 19011:2011,IDT)

GB/T 22080—2016　信息技术　安全技术　信息安全管理体系　要求(ISO/IEC 27001:2013,IDT)

GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2016,IDT)

3　术语和定义

GB/T 19011—2013和GB/T 29246—2017界定的术语和定义适用于本文件。

4　审核原则

GB/T 19011—2013的第4章审核原则适用。

5　审核方案的管理

5.1　总则

GB/T 19011—2013的5.1的指南适用。并且，以下ISMS特定的指南适用。

5.1.1　IS 5.1 总则

需要实施审核的组织宜建立审核方案，并考虑规划ISMS时所确定的风险和机会。

5.2　确立审核方案的目标

GB/T 19011—2013的5.2中的指南适用。并且，以下ISMS特定的指南适用。

5.2.1　IS 5.2 确立审核方案的目标

确立审核方案目标时，ISMS还宜考虑下列事项：

a) 确定的信息安全要求；

b) GB/T 22080—2016 的要求；

c) 发生信息安全事态和事件时所反映出的受审核方的绩效水平，以及 ISMS 的有效性；

注：有关绩效监视、测量、分析和评价的更多信息参见 GB/T 31497。

d) 规划 ISMS 时所确定的风险和机会；

e) 相关方的信息安全风险，例如受审核方和审核委托方。

ISMS 特定审核方案的目标可包括：

a) 相关法律、合同要求、其他要求及其安全影响的符合性验证；

b) 获得并保持对受审核方在风险管理能力方面的信心；

c) 评价应对信息安全风险和机会的措施的有效性。

5.3 建立审核方案

5.3.1 审核方案管理人员的作用和职责

GB/T 19011—2013 的 5.3.1 中的指南适用。

5.3.2 审核方案管理人员的能力

GB/T 19011—2013 的 5.3.2 中的指南适用。

5.3.3 确定审核方案的范围和详略程度

GB/T 19011—2013 的 5.3.3 中的指南适用。并且，以下 ISMS 特定的指南适用。

5.3.3.1 IS 5.3.3 确定审核方案的范围和详略程度

审核方案的范围和详略程度会有所不同，并受下列因素影响：

a) ISMS 规模，包括：

1) 在组织控制下开展工作的人员总数，以及与 ISMS 有关的相关方和合同方；

2) 信息系统的数量；

3) ISMS 覆盖的场所数量。

b) ISMS 的复杂程度（包括过程和活动的数量和关键性），并考虑 ISMS 范围内场所间的差异。

c) 与业务有关的信息安全风险的重要性。

d) 规划 ISMS 时所确定的风险和机会的重要性。

e) 在 ISMS 范围内保持信息的保密性、完整性和可用性的重要性。

f) 待审核信息系统的复杂度，包括所部署信息技术的复杂度。

g) 相似办公场所的数量。

宜在审核方案中确定优先事项，以便根据信息安全风险的重要性和 ISMS 范围内的业务要求开展更详细的审核。

注：关于确定审核时间的更多信息可在 GB/T 25067—2020 中找到。更多关于多场所抽样的信息可在 GB/T 25067—2020 和国际认可论坛的规范文件 1（IAF MD1，参考文献[15]）中找到。GB/T 25067—2020 和 IAF MD1 所包含的信息仅与认证审核有关。

5.3.4 识别和评估审核方案风险

GB/T 19011—2013 的 5.3.4 中的指南适用。并且，以下 ISMS 特定的指南适用。

5.3.4.1 IS 5.3.4 识别和评估审核方案风险

审核方案风险还可能涉及保密要求相关的风险。

5.3.5 建立审核方案的程序

GB/T 19011—2013 的 5.3.5 中的指南适用。并且，以下 ISMS 特定的指南适用。

5.3.5.1 IS 5.3.5 建立审核方案的程序

宜根据受审核方和其他相关方的要求确定信息安全和保密的保障措施。其他方要求包括相关的法律和合同要求。

5.3.6 识别审核方案资源

GB/T 19011—2013 的 5.3.6 中的指南适用。并且，以下 ISMS 特定的指南适用。

5.3.6.1 IS 5.3.6 识别审核方案资源

ISMS 审核员尤其宜分配足够的时间，针对适用于受审核方且与审核方案目标相关的所有重大风险，评审应对信息安全风险以及 ISMS 相关风险和机会所采取措施的有效性。

5.4 实施审核方案

5.4.1 总则

GB/T 19011—2013 的 5.4.1 中的指南适用。

5.4.2 规定每次审核的目标、范围和准则

GB/T 19011—2013 的 5.4.2 中的指南适用。并且，以下 ISMS 特定的指南适用。

5.4.2.1 IS 5.4.2 规定每次审核的目标、范围和准则

审核目标可包括以下内容：

a) 评价 ISMS 是否充分识别并解决信息安全要求；

b) 评价维护和有效改进 ISMS 的过程；

c) 确定信息安全控制对 ISMS 要求和规程的符合程度。

审核范围宜考虑到信息安全风险，以及相关方（即审核委托方和受审核方）对 ISMS 带来的风险和机会。

如果 ISMS 处于审核范围内，那么审核组宜根据内部和外部事项以及相关方的需求和期望，确认受审核方 ISMS 的范围和边界。审核组宜确认受审核方在 ISMS 范围内满足 GB/T 22080—2016 的 4.3 中规定的与审核范围有关的要求。

下列文件可作为审核准则，并用作确认符合性的参考：

a) 受审核方采用的信息安全方针、信息安全目标、策略和规程；

b) 法律和合同要求以及与受审核方相关的其他要求；

c) 受审核方的信息安全风险准则、信息安全风险评估过程以及风险处置过程；

d) 适用性声明，特定部门或其他必要控制的识别以及对包含必要的控制及其选择的合理性说明（无论该控制是否已实现），以及对 GB/T 22080—2016 附录 A 控制删减的合理性说明；

e) 可适当处置风险的控制的定义；

f) 监视、测量、分析和评价信息安全绩效及 ISMS 有效性的方法和准则；

g) 客户的信息安全要求；

h) 供应商或外包商应用的信息安全要求。

5.4.3 选择审核方法

GB/T 19011—2013 的 5.4.3 中的指南适用。并且，以下 ISMS 特定的指南适用。

5.4.3.1 IS 5.4.3 选择审核方法

如果进行联合审核，则宜特别关注相关方之间的信息泄露问题。在开始审核之前，宜与所有相关方达成协议。

5.4.4 选择审核组成员

GB/T 19011—2013 的 5.4.4 中的指南适用。并且，以下 ISMS 特定的指南适用。

5.4.4.1 IS 5.4.4 选择审核组成员

整个审核组的能力宜包括充分认识和理解：

a) 信息安全风险管理知识，足以支撑其评价受审核方所使用的方法；
b) 信息安全及信息安全管理知识，足以支撑其评价控制的确定以及 ISMS 的规划、实现、维护和有效性。

5.4.5 为审核组长分配每次的审核职责

GB/T 19011—2013 的 5.4.5 中的指南适用。

5.4.6 管理审核方案结果

GB/T 19011—2013 的 5.4.6 中的指南适用。

5.4.7 管理和保持审核方案记录

GB/T 19011—2013 的 5.4.7 中的指南适用。

5.5 监视审核方案

GB/T 19011—2013 的 5.5 中的指南适用。

5.6 评审和改进审核方案

GB/T 19011—2013 的 5.6 中的指南适用。

6 实施审核

6.1 总则

GB/T 19011—2013 的 6.1 中的指南适用。

6.2 审核的启动

6.2.1 总则

GB/T 19011—2013 的 6.2.1 中的指南适用。

6.2.2 与受审核方建立初步联系

GB/T 19011—2013 的 6.2.2 中的指南适用。并且，以下 ISMS 特定的指南适用。

6.2.2.1 IS 6.2.2 与受审核方建立初步联系

必要时，宜确保审核员获得使用文件化信息或审核活动所需其他信息（包括但不限于涉密或敏感信息）的必要安全许可。

6.2.3 确定审核的可行性

GB/T 19011—2013 的 6.2.3 中的指南适用。并且，以下 ISMS 特定的指南适用。

6.2.3.1 IS 6.2.3 确定审核的可行性

在审核开始之前，审核员宜询问受审核方是否存在无法提供审核组评审的 ISMS 审核证据，例如，因为证据中包含了个人身份信息或其他涉密/敏感信息。负责管理审核方案的人员宜确定在缺少这部分审核证据的情况下是否仍可对 ISMS 进行充分审核。如果得出的结论为缺少对这部分审核证据的评审将导致无法充分审核 ISMS，负责管理审核方案的人员宜告知受审核方，在获得适当的准入安排或向受审核方提出或实施审核的替代手段之前，审核将无法进行。如果审核继续进行，审核计划宜考虑到所有访问限制。

6.3 审核活动的准备

6.3.1 审核准备阶段的文件评审

GB/T 19011—2013 的 6.3.1 中的指南适用。

6.3.2 编制审核计划

GB/T 19011—2013 的 6.3.2 中的指南适用。并且，以下 ISMS 特定的指南适用。

6.3.2.1 IS 6.3.2 编制审核计划

审核组长宜意识到审核组成员在现场可能对受审核方造成的风险。审核组在现场可能会影响受审核方的信息安全，产生额外的风险源，例如涉密或敏感记录或系统基础设施（例如意外删除、未授权信息泄露、无意的信息变更）。

6.3.3 审核组工作分配

GB/T 19011—2013 的 6.3.3 中的指南适用。

6.3.4 准备工作文件

GB/T 19011—2013 的 6.3.4 中的指南适用。并且，以下 ISMS 特定的指南适用。

6.3.4.1 IS 6.3.4 准备工作文件

审核组长宜确保所有审核工作文件得以适当分类和处理。

6.4 审核活动的实施

6.4.1 总则

GB/T 19011—2013 的 6.4.1 中的指南适用。

6.4.2 举行首次会议

GB/T 19011—2013 的 6.4.2 中的指南适用。

6.4.3 审核实施阶段的文件评审

GB/T 19011—2013 的 6.4.3 中的指南适用。并且，以下 ISMS 特定的指南适用。

6.4.3.1 IS 6.4.3 审核实施阶段的文件评审

ISMS 审核员宜验证审核准则所要求的且与审核范围相关的文件化信息是否存在，并符合审核准则要求。

ISMS 审核员宜确认审核范围内所确定的控制与风险评估和风险处置结果相关，并可追溯到信息安全方针和目标。

注：附录 A 为 ISMS 审核实践提供指南，包括如何使用相关文件化信息审核 ISMS。

6.4.4 审核中的沟通

GB/T 19011—2013 的 6.4.4 中的指南适用。

6.4.5 向导和观察员的作用和责任

GB/T 19011—2013 的 6.4.5 中的指南适用。

6.4.6 信息的收集和验证

GB/T 19011—2013 的 6.4.6 中的指南适用。并且，以下 ISMS 特定的指南适用。

6.4.6.1 IS 6.4.6 信息的收集和验证

在审核过程中收集相关信息的方法可包括：

a) 核查记录(包括计算机日志和配置数据)；

b) 访问信息处理设备；

c) 观察 ISMS 过程以及已实现的相关控制；

d) 使用自动审核工具。

注 1：附录 A 提供了关于如何审核 ISMS 过程的指南。

注 2：GB/Z 32916 提供了如何评价信息安全控制的额外指南。

ISMS 审核组成员宜根据审核委托方、审核组和受审核方之间的协议，确保从受审核方获取的所有信息得到适当处理。

6.4.7 形成审核发现

GB/T 19011—2013 的 6.4.7 中的指南适用。

6.4.8 准备审核结论

GB/T 19011—2013 的 6.4.8 中的指南适用。

6.4.9 举行末次会议

GB/T 19011—2013 的 6.4.9 中的指南适用。

6.5 审核报告的编制和分发

6.5.1 审核报告的编制

GB/T 19011—2013 的 6.5.1 中的指南适用。并且，以下 ISMS 特定的指南适用。

6.5.1.1 IS 6.5.1 审核报告的编制

如果审核组在审核过程中由于信息级别或敏感原因无法获得审核证据，则审核组长宜判断其影响审核发现和结论可信度的程度，并在审核报告中予以反映，不能因证据敏感性导致其不可用而进行妥协。

6.5.2 审核报告的分发

GB/T 19011—2013 的 6.5.2 中的指南适用。并且，以下 ISMS 特定的指南适用。

6.5.2.1 审核报告的分发

在分发审核报告时，宜采取适当措施确保报告的保密性。

注：当使用电子方式进行分发时，可适当加密审核报告。

6.6 审核的完成

GB/T 19011—2013 的 6.6 中的指南适用。

6.7 审核后续活动的实施

GB/T 19011—2013 的 6.7 中的指南适用。

7 审核员的能力和评价

7.1 总则

GB/T 19011—2013 的 7.1 中的指南适用。

7.2 确定满足审核方案需求的审核人员能力

7.2.1 总则

7.2.1.1 总则

GB/T 19011—2013 的 7.2.1 中的指南适用。并且，以下 ISMS 特定的指南适用。

7.2.1.2 IS 7.2.1 总则

在确定 ISMS 审核员的适当知识和技能时，宜考虑以下内容：

a) ISMS 的复杂度(例如 ISMS 内信息系统的重要性，ISMS 的风险评估结果)；
b) 在 ISMS 范围内开展的业务类型；
c) 实现 ISMS 各组成部分(例如实现的控制、文件化信息和/或过程控制、涉及的技术平台和解决方案等)所使用技术的范围和多样性；
d) 之前已证实的 ISMS 的绩效；
e) ISMS 范围内所用的外部方以及外包程度；
f) 与审核方案相关的标准、法律要求和其他要求。

7.2.2 个人行为

GB/T 19011—2013 的 7.2.2 中的指南适用。

7.2.3 知识和技能

7.2.3.1 总则

GB/T 19011—2013 的 7.2.3.1 中的指南适用。

7.2.3.2 管理体系审核员的通用知识和技能

GB/T 19011—2013 的 7.2.3.2 中的指南适用。

7.2.3.3 管理体系审核员的特定领域与专业的知识和技能

GB/T 19011—2013 的 7.2.3.3 中的指南适用，并且 GB/T 19011—2013 中 A.7 的指南也适用。

7.2.3.4 审核组长的通用知识和技能

GB/T 19011—2013 的 7.2.3.4 中的指南适用。

7.2.3.5 多领域管理体系审核的知识和技能

GB/T 19011—2013 的 7.2.3.5 中的指南适用。

7.2.4 审核员能力的获得

7.2.4.1 总则

GB/T 19011—2013 的 7.2.4 中的指南适用。并且，以下 ISMS 特定的指南适用。

7.2.4.2 IS 7.2.4 审核员能力的获得

ISMS 审核员宜具备信息技术和信息安全方面的知识和技能，如通过相关认证（例如基于 GB/T 27024认可的认证）。ISMS 审核员也宜理解相关业务需求。ISMS 审核员的个人工作经验宜对他们在 ISMS 领域的知识和技能有所帮助。

注：有关 ISMS 审核员认证的更多信息可在 GB/T 25067—2020 中找到。

7.2.5 审核组长

GB/T 19011—2013 的 7.2.5 中的指南适用。

7.3 审核员评价准则的建立

GB/T 19011—2013 的 7.3 中的指南适用。

7.4 选择适当的审核员评价方法

GB/T 19011—2013 的 7.4 中的指南适用。

7.5 进行审核员评价

GB/T 19011—2013 的 7.5 中的指南适用。

7.6 保持并提高审核员能力

GB/T 19011—2013 的 7.6 中的指南适用。

附 录 A
（资料性附录）
ISMS 审核实践指南

A.1 概述

本附录对声称符合 GB/T 22080—2016 的组织提供审核 ISMS 的通用指南。由于本附录旨在适用于所有 ISMS 审核，所以无论涉及的组织是何规模或性质，本附录均适用。本附录旨在供开展 ISMS 内部或外部审核的审核员使用。

注：GB/T 31496—2015 根据 GB/T 22080—2016 给出了实施和操作 ISMS 的指南。

A.2 总则

A.2.1 审核目标、范围、准则和审核证据

在审核活动期间，宜通过适当的抽样方式获得并验证与审核目标、范围和准则有关的信息，包括职责，活动和过程之间的接口相关信息。只有可证实的信息才可作为审核证据。宜记录导致审核发现的审核证据。

获取信息的方法包括以下内容：

——访谈；

——观察；

——文件评审，包括记录。

A.2.2 ISMS 审核策略

GB/T 22080—2016 遵循 ISO/IEC 导则第 1 部分附录 JC 和融合的 JTC1 补充部分中的顶层结构、相同的章条标题、核心文本、通用术语与核心定义——JTC1 特定规程。GB/T 22080—2016 定义了一组相互依赖的要求，这些要求作为一个整体发挥作用（通常被称为“体系方法”），并通过交叉引用予以部署。

在审核时最好同时处理实践中密切相关的 GB/T 22080—2016 章条。相关示例见表 A.2。

例如 GB/T 22080—2016 中 6.1.3 和 8.3 以及 6.2、5.1、5.2、5.3、7.1、7.4、7.5、9.1、9.3 和 10.2，同时审核这些章条及其关联或相关章条才有意义。

GB/T 22080—2016 中 7.5 提出了有关文件化信息的要求。如表 A.2 中 A.4.5 所述，每次审核员检查一份文件化信息时，都是确认其是否符合 GB/T 22080—2016 中 7.5 要求的机会。有关如何执行上述内容的指南在表 A.2 的 A.4.5 中。表中每次出现“文件化信息”时，将不再重复对文件化信息的要求。

A.2.3 审核和文件化信息

审核活动涉及文件化信息，即：

a) 在 GB/T 22080—2016 中文件化信息的要求章条可用作审核准则；

b) 以下文件化信息可作为审核证据：

1) GB/T 22080—2016 的 7.5.1 a)中要求的文件化信息；

2) 由组织确定的，GB/T 22080—2016 的 7.5.1 b)中要求的 ISMS 有效运行所必需的文件化信息。

除 A.2.3 b)中所列的审核证据，审核员将通过访谈、观察和文件评审（包括记录）获得其他审核

证据。

有关 GB/T 22080—2016 的文件化信息的详细讨论可在 A.3 中找到。

A.3 GB/T 22080—2016 文件化信息要求指南

A.3.1 基本原理

审核员提出要求将文件化信息作为符合性证据时宜注意：

a) 表 A.1 中所列的对文件化信息的 16 项明确要求，包括适用性声明；

b) 其他要求：

1) 可从 a)中所述文件化信息中找出符合性证据；

2) 文件化信息未体现显性或隐性要求。

表 A.1 GB/T 22080—2016 中对文件化信息的要求

有关的文件化信息要求	参考 GB/T 22080—2016 章条号
ISMS 的范围	4.3
信息安全策略	5.2
信息安全风险评估过程	6.1.2
信息安全风险处置过程	6.1.3
适用性声明	6.1.3 d)
信息安全目标	6.2
能力的证据	7.2 d)
由组织确定的有效实施 ISMS 所必需的文件化信息	7.5.1 b)
运行规划和控制	8.1
信息安全风险评估的结果	8.2
信息安全风险处置的结果	8.3
监视和测量结果的证据	9.1
审核方案和审核结果的证据	9.2 g)
管理评审结果的证据	9.3
表明不符合的性质以及后续措施的证据	10.1 f)
任何纠正措施结果的证据	10.1 g)

注：审核的定义表明它是一个文件化的过程，因此审核员可认为 GB/T 22080—2016 的 9.2 要求的结果是一个文件化的审核过程。

A.3.2 对文件化信息有隐性要求的示例

作为 A.3.1 b)1)的一个示例，在 GB/T 22080—2016 的 6.1.2 中要求组织“保留有关信息安全风险评估过程的文件化信息”。在这条之前的要求[GB/T 22080—2016 的 6.1.2 a)～e)]均涉及风险评估过程。因此，符合上述要求的证据存在于所要求的风险评估过程相关文件化信息中。

A.3.3 文件化信息未体现显性或隐性要求的示例

作为 A.3.1 b)2)的一个示例，考虑 GB/T 22080—2016 的 4.1 要求。对外部和内部事项相关的信息

未要求文件化。因此，审核员不宜要求看到相关文件化信息。然而，如果组织不能解释其已对这些问题进行决策，将构成对 GB/T 22080—2016 的 4.1 的不符合。但是，组织有责任确定证明其符合要求的方式。证明方式包括最高管理者的解释(即有人知悉)；在会议中讨论过该主题；在正式配置管理下的文件化信息中得到证明；也可通过其他方式证明。实际上，证据很可能会分散在 ISMS 的文件化信息中。例如，GB/T 22080—2016 的 4.1 的目的是帮助组织理解其 ISMS 环境。该环境贯穿于整个 ISMS，尤其是在确定范围、方针以及执行风险评估和风险处置过程时。如果组织符合 GB/T 22080—2016 中 4.1 的要求，其外部和内部事项的知识可能会应用于 ISMS 的其他领域，这些应用将保持一致，并可能会有这些领域文件化信息的符合证据。

A.4 适用性声明

适用性声明(SOA)是另一个需要注意的领域。SOA 宜包含所有必要的控制，即组织已有的控制、作为风险处置过程[GB/T 22080—2016 中 6.1.3 c)]结果的控制(为满足风险接受准则而对信息安全风险进行修改所需的控制)。所有必要的控制均为组织自身的要求。

必要的控制可能是 GB/T 22080—2016 附录 A 中的控制(非强制要求)，也可能来自其他标准(例如 ISO/IEC 27017)或其他来源，或者由组织进行专门设计。

在某些情况下，组织所使用的控制对 GB/T 22080—2016 附录 A 中的控制进行了变更，删减了 GB/T 22080—2016 附录 A 中的控制，删减的理由是它已被组织变更后的控制所代替。其实这种变更可能并入 GB/T 22080—2016 附录 A 的控制中，不作为删减。

审核员宜基于组织各类必要的控制规范来判定符合性，而无需依据 GB/T 22080—2016 附录 A 给出的规范。如果组织的规范要求一个文件化规程，这会形成组织对 GB/T 22080—2016 中 7.5.1b)的部分符合。如果未要求有文件化规程，那么审核员不宜要求见到该规程。但是，审核员宜关注(GB/T 22080—2016 中 8.1)中的要求，组织宜“保持文件化信息达到必要的程度，以确信这些过程按计划得到执行”。鉴于 GB/T 22080—2016 中 8.1 引用了 GB/T 22080—2016 中 6.1 的内容，组织的风险处置计划及其必要的控制，都在文件化信息要求的范围内。

在审核控制的选择时，最好针对风险处置计划进行审核[如 GB/T 22080—2016 的 6.1.3 e)中所述]，而不只是审核适用性声明中所列出的个别必要控制。风险处置计划可能详细说明了必要控制之间的相互作用，而仅使用适用性声明则可能忽略这个因素。

A.5 其他文件化信息

GB/T 22080—2016 的关注焦点是结果。在文件化信息的 16 个明确要求中(见表 A.1)，只有三个涉及的规范(信息安全风险评估过程、信息安全风险处置过程和审核方案)。但是，这并不妨碍组织拥有文件化的规程。此类支持文件属于 GB/T 22080—2016 中 7.5.1 b)的范围(组织确定的文件化信息对其 ISMS 的有效性是必要的)。因此，这类文件作为组织的要求，宜包含在审核范围内。

A.6 注释

所需信息可能是网页的一部分，或作为数据库查询的结果呈现给阅读人员。此外，除了适用性声明以外，GB/T 22080—2016 未给出文件名称。因此，有关信息安全策略的文件化信息可能不在名为“信息安全策略”的文件或网页中。组织有权为信息安全策略定义其他名称。在确保 ISMS 符合 GB/T 22080—2016 的 5.3 a)要求方面具备责任和权限的人员是相同的，都宜知悉 GB/T 22080—2016 中强制要求的文件化信息与他们的文件化信息之间的关系。

A.7 ISMS 审核指南

表 A.2 列出了以下信息：

——相应的 GB/T 22080—2016 章条编号和名称；

——相关章条(有关如何使用此行的信息，请参阅 A.2.2)；

——GB/T 22080—2016 相应的章条在 GB/T 29246 中的相关定义；

——“审核证据”，可能来源于 GB/T 22080—2016 的相应章条；

——“审核实践指南”，即审核的指南(参见 A.3)；

——“支持性文件”，针对相应的 GB/T 22080—2016 章条参考对审核有帮助的其他文件。

表 A.2 GB/T 22080—2016 的审核指南

A.1 组织环境(4)	
A.1.1 理解组织及其环境(4.1)	
GB/T 22080—2016 中相关章条	6.1、9.3
GB/T 29246 中相关定义	外部环境、信息安全、内部环境、管理体系、组织
审核证据	审核证据可通过以下方面的文件化信息或其他信息获得： a) 可能对 ISMS 产生积极或消极影响的重要事项； b) 组织； c) 组织的目的； d) ISMS 的预期结果。 重要事项的可能来源包括： a) 与气候、污染、资源可用性和生物多样性有关的环境特性或情况，以及这些情况可能对组织实现其目标的能力产生的影响。 b) 来自于国际、国内、地区、当地的各种外部文化的、社会的、政治的、法律的、监管的、金融的、技术的、经济的、自然的和竞争的环境。 c) 组织的特征或条件，例如组织管理、信息流和决策过程： ——组织的政策、目标和实现它们的战略； ——组织的文化； ——组织采用的标准、准则和模型； ——组织产品和服务的生命周期； ——信息系统、过程、科学和技术的潜在信息安全管理。 d) 审核和风险评估的趋势
审核实践指南	审核员宜确认该组织： a) 有对可能积极或消极影响 ISMS 的重要事项有一个高层次(例如战略的)的理解； b) 了解与其目的相关的外部和内部事项，以及影响其实现 ISMS 预期结果能力的事项。 注 1：4.3 中的要求是“考虑 4.1 中提到的外部和内部事项”。组织可考虑在输出中未出现的内容。 审核员还宜确认通过应用风险管理过程使风险得到充分管理，来保护信息的保密性、完整性和可用性的预期结果。 审核员还宜验证：组织重要主题、辩论和讨论的问题以及变化的环境等相关事项的知识，是否被确认已用于指导组织规划、实现和运行管理体系

表 A.2（续）

支持性文件	ISO/IEC 导则第 1 部分:2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000:2009 的 5.3 ISO/IEC 27003:2017 的 4.1
A.1.2 理解相关方的需求和期望(4.2)	
GB/T 22080—2016 中相关章条	4.1、4.3
GB/T 29246 中相关定义	相关方
审核证据	审核证据可通过下列文件化信息或其他信息获得： a) 相关方； b) 适用于 ISMS 和 GB/T 22080—2016 的相关方的需求和期望。 **注 2**：潜在的相关方可能包括： a) 法律和监管机构(当地、地区、自治区/省、国家或国际)； b) 上级组织； c) 客户； d) 贸易和专业协会； e) 社区团体； f) 非政府组织； g) 供应商； h) 邻居； i) 组织成员和代表组织工作的其他人； j) 信息安全专家。 **注 3**：相关方要求可能包括： a) 法律； b) 许可、执照或其他形式的授权； c) 监管机构发布的决议； d) 法院或行政法庭的判决； e) 条约、公约和议定书； f) 相关行业规范和标准； g) 已签订的合同； h) 与社区团体或非政府组织达成的协议； i) 与公共机构和客户的协议； j) 组织要求； k) 自愿性原则或行为守则； l) 自愿性标识或环境承诺； m) 根据与该组织的合同安排产生的义务； n) 信息和通信交换。 **注 4**：相关方可能有不同的利益，这些利益可能完全一致、部分一致或与组织的经营目标相对立。与组织的经营目标相对立的相关方示例为黑客。黑客要求组织形成弱安全性。组织宜重视这类完全对立的相关方需求，即加强安全性。 审核员宜意识到 ISMS 考虑了所有内部和外部风险源。因此，组织对相对立的相关方及其需求的理解具有高度相关性

表 A.2（续）

审核实践指南	审核员宜确认组织对适用于 ISMS 和 GB/T 22080—2016 的相关方的需求和期望有一个高层次（如战略性）的理解。 审核员宜核实该组织是否已识别出相关方的需求，包括自愿采纳或签订的协议、合同，或因纳入法律、法规、许可、政府授权或法庭诉讼中所导致的强制性需求和期望。值得注意的是，并非所有相关方要求都是组织的要求，有些要求不适用于组织或与 ISMS 不相关。一些相关方的需求（例如黑客的需求）与 ISMS 的目的相反，组织宜通过适当的信息安全控制来确保这些需求和期望不会被满足。 审核员还可确认是否有相关方意识到他们会受到 ISMS 的影响，如果是的话，他们需让组织知道这些情况。 审核员还可验证组织是否使用所获得的知识来指导其规划、实现和运行 ISMS 的工作
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000：2009 的 5.3 ISO/IEC 27003：2017 的 4.2
A.1.3 确定 ISMS 范围（4.3）	
GB/T 22080—2016 中相关章条	4.1、4.2
GB/T 29246 中相关定义	外包
审核证据	审核证据可通过以下文件化信息或其他信息获得： ——组织管理体系的范围（4.3 中定义）； ——适用时，组织的认证范围； ——适用性声明。 **注 5**：组织认证的范围不一定与其 ISMS 的范围相同。通常情况下，认证范围仅限于 ISMS 组织架构。
审核实践指南	审核员宜确认组织根据自己的意愿确定应用 ISMS 的物理、信息、法律和组织边界，并选择在整个组织内还是在组织内的特定部门或职能部门实现 GB/T 22080—2016。 审核员宜核实组织对其环境（4.1）、相关方（4.2）的要求以及组织执行的活动和其他组织执行的活动之间的接口和依赖性[4.3 c)]的理解，并在确定 ISMS 的范围时予以充分考虑。 审核员宜进一步确认组织的信息安全风险评估和风险处置恰当地反映了其活动，并延伸到 ISMS 范围内定义的活动边界，再延伸到适用的审核范围。审核员宜核实每一个审核范围内至少有一个适用性声明，并且在适用性声明中包含了风险管理过程中确定的所有控制。这些控制是指 GB/T 22080—2016 中 6.1.3 b）所述的必要控制，不必是 GB/T 22080—2016 附录 A 中所述的控制。这些控制可包括适用于特定行业的控制，以及组织自行设计或从其他来源识别的控制。 审核员还宜确认不完全在 ISMS 范围内的服务或活动的接口在 ISMS 中得到解决，并包含在组织的信息安全风险评估中。例如与其他组织共享设施（例如 IT 系统、数据库、远程通信系统或业务功能的外包）。 宜确认已建立范围文件，并根据文件化信息（7.5）的要求进行控制
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000：2009 的 5.3 ISO/IEC 27003：2017 的 4.3 GB/T 25067—2020 的 8.2、9.1.3.5 GB/T 27021.1—2017 的 8.2.2

表 A.2（续）

A.1.4 信息安全管理体系（4.4）	
GB/T 22080—2016 中相关章条	6.1.1、6.1.2、6.1.3、8.1、8.2、8.3
GB/T 29246 中相关定义	持续改进、信息安全、管理体系
审核证据	审核证据可通过 GB/T 22080—2016 要求建立的文件化信息或其他过程信息获得，包括： a) 管理体系的过程(GB/T 22080—2016 的 4.4)； b) 业务规划和控制过程，包括外包过程(8.1)； c) 规划 ISMS 时应对风险和机会的过程，包括信息安全风险评估过程(6.1.2 和/或 8.2)和信息安全风险处置过程(6.1.3 和/或 8.3)； d) 实现信息安全目标的过程
审核实践指南	审核员宜核实组织创建了“必要且充分”的一组过程和控制，这些过程和控制共同构成了符合 GB/T 22080—2016 的有效的管理体系，并建立了由相互关联或相互作用的要素构成的 ISMS。 审核员还宜确认，该组织在目前的能力范围内保持了决定如何满足 ISMS 要求的权力、义务和自主权，包括详略程度及将 ISMS 要求纳入其业务的程度
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000：2009 的 5.3 ISO/IEC 27003：2017 的 4.4
A.2 领导(5)	
A.2.1 领导和承诺（5.1）	
GB/T 22080—2016 中相关章条	4.1、4.2、4.4、5.2、5.3、6.1.1、6.2、7.1、7.4、8.1、9.3、10.2
GB/T 29246 中相关定义	信息安全、最高管理者
审核证据	审核证据可通过以下方面的文件化信息或其他信息获得： a) 信息安全方针[GB/T 22080—2016 的 5.1 a)]； b) 信息安全目标[5.1 a)]； c) 组织的过程； d) 管理评审的结果[5.1 c]、e)和 g)]； e) 评估资源需求； f) 有效的信息安全管理的重要性和遵守 ISMS 要求的沟通。 还可通过与最高管理者的访谈获得证据。管理评审的结果还可提供除 5.1 c)、e)和 g)以外的子章条的审核证据

表 A.2（续）

审核实践指南	审核员宜确认组织最高管理者的强力支持、参与和承诺，这对成功实现 GB/T 22080—2016 非常重要。 审核员还宜审核： a) 已定义的最高管理者的职责； b) 最高管理者对分配给组织的活动的圆满完成负有责任； c) 最高管理者确保建立信息安全方针和目标，并与组织战略方向一致； d) 最高管理者传达有效的信息安全管理和符合 ISMS 要求的重要性； e) 最高管理者通过支持所有信息安全管理过程的实现，特别是通过要求和评审有关 ISMS 状态和有效性的报告[见 5.3 b)]，确保 ISMS 达到其预期结果； f) 最高管理者指导并支持组织中直接参与信息安全和 ISMS 的人员； g) 最高管理者确保将 ISMS 要求整合到组织过程中； h) 最高管理者确保 ISMS 所需资源可用； i) 最高管理者在管理评审时评估资源需求，并设定持续改进和监视计划活动有效性的目标； j) 最高管理者创建文化和环境氛围，鼓励员工积极努力实现 ISMS 要求，并争取实现信息安全目标
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000：2009 的 4.2 ISO/IEC 27003：2017 的 5.1
A.2.2 方针(5.2)	
GB/T 22080—2016 中相关章条	6.2、7.4
GB/T 29246 中相关定义	信息安全、方针
审核证据	审核证据可通过以下文件化信息或其他信息获得： a) 信息安全方针(5.1)； b) 信息安全目标[5.2 b)和 6.2]
审核实践指南	审核员宜确认： a) 信息安全方针说明了 GB/T 22080—2016 要求的高层次的组织承诺，并考虑了组织的目标； b) 信息安全方针用于构建或建立组织为自己设定的信息安全目标，或明确说明为信息安全策略的一部分； c) 信息安全方针的文件化信息是根据文件化信息(7.5)的要求建立和控制的； d) 信息安全方针按照沟通章条(7.4)的要求在内部得到沟通； e) 信息安全方针适当时对其他相关方可用。 由于信息安全方针包含了满足适用要求的承诺，特别是相关法律法规要求。因此，只要对导致不符合的系统缺陷及时发现并采取纠正措施，即不宜视为不符合
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000：2009 的 4.3.2 ISO/IEC 27003：2017 的 5.2
A.2.3 组织的角色、责任和权限(5.3)	
GB/T 22080—2016 中相关章条	7.4、9.2、9.3

表 A.2（续）

GB/T 29246 中相关定义	信息安全、组织、最高管理者
审核证据	参考 GB/T 22080—2016 的 7.5.1 b)，审核证据可通过以下方面的文件化信息或其他信息获得： a) 组织的角色； b) 在信息安全控制下工作并对组织的信息安全绩效产生影响的人员的岗位说明书； c) 执行内部审核方案及审核结果； d) ISMS 的范围与组织架构。 此外，还可通过管理评审结果的文件化信息或其他信息来开展进一步的审核
审核实践指南	审核员宜通过审核文件化信息和/或访谈确认： a) 执行 ISMS 要求的职责和权限被分配给组织内的相关角色； b) 最高管理者负责这些职责和权限被分配并传达给执行这些角色的人员； c) 按照沟通章条(7.4)的要求沟通职责和权限； d) 按照内部审核(9.2)的要求实施，证明符合 GB/T 22080—2016 的要求； e) 按照管理评审(9.3)的要求实施绩效的报告。 审核员宜验证有责任的人员是否有足够的权限与最高管理者联系，以便其了解 ISMS 的状态和绩效。 注 6：确保管理体系符合 GB/T 22080—2016 要求的角色可分配到个人、由多个人共同承担或分配给团队
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000：2009 的 4.3.3 ISO/IEC 27003：2017 的 5.3
A.3 规划（6）	
A.3.1 应对风险和机会的措施（6.1）	
A.3.1.1 总则(6.1.1)	
GB/T 22080—2016 中相关章条	4.1、4.2、8.1、9、10.2
GB/T 29246 中相关定义	信息安全、风险、风险管理
审核证据	审核证据可通过以下文件化信息或其他信息获得： a) ISMS 的规划[GB/T 22080—2016 的 6.1.1、7.5.1 b)和 8.1]； b) 信息安全风险评估过程(6.1.2)； c) 信息安全风险评估结果(8.2)； d) 信息安全风险处置过程(6.1.3)； e) 信息安全风险处置结果(8.3)； f) 监视和测量结果(9.1)； g) 内部审核方案和内部审核结果(9.2)； h) 管理评审(9.3)； i) 组织环境(4)； j) 信息安全目标(6.2)

表 A.2（续）

审核实践指南	审核员宜确认规划： a) 在适当的水平上建立 ISMS； b) 考虑(4.1)中确定的组织环境相关的事项以及(4.3)中确定组织的适用要求，以解决 GB/T 22080—2016 中 6.1.1a)～c)有关的任何负面或正面的后果； c) 预期了潜在的情况和后果，从而在事前预防不良影响； d) 处置组织所确定的预期结果[6.1.1 a)]，包括通过应用风险管理过程保护信息的保密性、完整性和可用性； e) 通过目标设定(6.2)、运行控制(8.1)或 GB/T 22080—2016 的其他具体章条，例如资源规定(7.1)、能力(7.2)、信息安全风险评估(8.2)、信息安全风险处置(8.3)，确定如何将必要或有益的行动纳入到 ISMS 中； f) 确定评估所采取措施有效性的机制，包括监视、测量技术(9.1)、内部审核(9.2)或管理评审(9.3)
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000：2009 的 5.3～5.7 ISO/IEC 27003：2017 的 6.1.1
A.3.1.2 信息安全风险评估（6.1.2）	
GB/T 22080—2016 中相关章条	8.2
GB/T 29246 中相关定义	可用性、保密性、信息安全、完整性、风险接受、风险分析、风险评估、风险准则、风险识别
审核证据	审核证据可通过以下方面的文件化信息或其他信息获得： a) ISMS 规划 [GB/T 22080—2016 的 6.1.1、7.5.1 b)和 8.1]； b) 信息安全风险评估过程(6.1.2)和信息安全风险评估结果(8.2)
审核实践指南	审核员宜确认信息安全风险评估： a) 确定与 ISMS 相关的信息安全风险； b) 包括风险识别、风险分析和风险评估过程
	风险准则[GB/T 22080—2016 的 6.1.2 a)]
	审核员宜确认组织已建立并持续维护风险接受准则以及信息安全风险评估实施准则。虽然组织可自行考虑与风险准则相关的任何因素，包括风险接受准则和信息安全风险评估实施准则，但审核员宜评估组织是否基于已形成的决策建立了风险准则，包括风险接受准则和风险评估实施准则。 比较合理的是，组织的风险准则包含在风险评估过程的文件化信息中。如果没有，组织宜能向审核员解释它们是什么。至少，它们宜包括组织的风险接受准则和风险评估实施准则。 注 7：GB/T 22080—2016 的 8.2 要求组织在计划的时间间隔内、重大变更提出或发生时进行信息安全风险评估。可对所有 ISMS 或部分 ISMS 进行风险评估(例如当重大变更对 ISMS 的部分产生影响时，就要求对该部分进行新的风险评估)
	结果的一致性、有效性和可比较性 [GB/T 22080—2016 的 6.1.2 b]]

表 A.2（续）

审核实践指南	审核员宜确认信息安全风险评估产生一致的、有效的和可比较的结果。可通过以下方式执行： ——询问组织为何其自身的信息安全风险评估结果为一致的、有效的和可比较的； ——对有关信息安全风险评估结果的文件化信息进行抽样检查。 为了评估一致性和可重复性，审核员可验证： ——以同样方式评估类似情况下的类似风险； ——所评估风险的差异具有合理的理由； ——整体评估结果可清晰解释。 为了评估可比较性，审核员可验证： ——在以前的风险评估中相同风险是如何评价的，如果风险已经发生变化，是否可解释； ——如果一个风险高于或低于其他风险是可清晰进行解释的
	风险识别[GB/T 22080—2016 的 6.1.2 c)]
	审核员宜确认组织已识别出 ISMS 范围内与信息保密性、完整性和可用性丧失相关的信息安全风险。 **注 8**：GB/T 22080—2016 不要求仅通过资产、威胁和脆弱性来识别风险。其他风险识别方法也可接受，例如通过考虑事态和后果来识别风险。 可在组织有关风险评估的文件化信息中找到风险识别过程的描述（见下文）。 组织在制定风险识别方法时可考虑（非必需）的因素包括： a) 如何发现、识别和描述风险； b) 考虑的风险来源。 组织可考虑（非必需）的其他因素包括： a) 风险如何产生、增强、预防、降低、加速或延迟组织实现其信息安全目标；风险与机会相关，但非追求机会； b) 风险来源是否在组织的控制下，即使风险来源或原因可能不明显； c) 检查特定后果的连锁效应，包括级联效应和累积效应； d) 考虑各种后果，即使风险来源或产生原因不明显； e) 考虑可能的原因和情景，以显示可能发生的后果； f) 考虑所有重大原因和后果； g) 如何建立全面的风险列表。 **注 9**：发现无意中遗漏了大量必要的控制可能表明风险识别过程较弱。 宜通过抽样确认 ISMS 范围内的所有重要信息都包含在风险评估中。 审核员宜验证在风险评估结果的文件化信息中已识别出 ISMS 范围内与信息保密性、完整性和可用性丧失相关的风险。组织的信息安全目标可帮助审核员识别信息安全风险。 审核员还宜确认： a) 对于每种风险，已确定风险责任人； b) 每个风险责任人都有责任和权力来管理他们已识别的风险
	风险分析[GB/T 22080—2016 的 6.1.2 d)]

表 A.2（续）

审核实践指南	审核员宜确认： a) 组织宜理解所识别风险的性质，确定风险的级别，作为信息安全风险评估过程中风险分析的依据； b) 风险分析为风险评价、风险需如何处置及最适当的风险处置、战略和方法方面的决策提供输入。 审核员还宜确认组织已评估了其根据 GB/T 22080—2016 的 6.1.2 c)所确定风险的潜在后果和可能性，从而确定风险级别。 可在关于风险评估过程的文件化信息中找到组织风险分析方法的描述，结果将出现在关于风险评估结果的文件化信息中(见下文)。审核员宜参考组织的风险管理策略、战略和方法。 风险分析可： a) 根据风险、分析目的以及可用的信息、数据和资源，以不同详略程度开展； b) 定性、半定量、定量或这些方法的组合，依环境而定
	风险评价[GB/T 22080—2016 的 6.1.2 e)]
	审核员宜确认组织已将其风险分析结果与信息安全风险接受准则进行比较，以确定已识别风险的可接受性。 审核员还宜确认在风险评估结果中，可表明风险接受准则已得到适当应用，且所识别和分析的风险已被优先处置。 进一步，审核员宜评审风险评估： a) 根据风险分析的结果，协助制定风险处置的方式和处置实施的优先顺序； b) 涉及将分析过程中发现的风险水平与考虑背景时建立的信息安全风险准则进行比较。 审核员还宜评估决定： a) 考虑更广泛的风险背景； b) 考虑相关利益方的要求，包括法律、监管和其他要求
	文件化信息(GB/T 22080—2016 的 6.1.2 和 8.2)
	审核员宜确认存在关于风险评估过程的文件化信息。 关于信息安全风险评估过程的文件化信息包括： a) 风险准则的定义，包括风险接受准则和信息安全风险评估实施准则； b) 结果的一致性、有效性和可比较性的基本原理； c) 风险识别过程的描述(包括风险责任人的识别)； d) 分析信息安全风险过程的描述(包括评估潜在后果、现实可能性及由此建立的风险水平)； e) 结果与风险准则进行比较的描述，以及风险处置优先级的描述。 注 10：上述各项均符合 GB/T 22080—2016 要求，这就是为什么可在关于风险评估过程的文件化信息中找到相关信息的原因
支持性文件	ISO 31000:2009 的 5.3、5.4、5.7 ISO/IEC 27003:2017 的 6.1.2、8.2
A.3.1.3 信息安全风险处置(6.1.3)	
GB/T 22080—2016 中相关章条	8.3、附录 A

表 A.2（续）

GB/T 29246 中相关定义	控制、控制目标、文件化信息、信息安全、残余风险、风险评估、风险准则、风险责任人、风险处置
审核证据	审核证据可通过以下方面的文件化信息或其他信息获得： a) ISMS 规划； b) 信息安全风险处置过程； c) 信息安全风险处置结果； d) 适用性声明
审核实践指南	**信息安全风险处置（GB/T 22080—2016 的 6.1.3）**
	审核员宜确认组织将信息安全风险修改作为了信息安全风险处置过程。 审核员还宜评审信息安全风险处置是否涉及： a) 选择一个或多个选项来修改信息安全风险，并实现这些规定或修改控制的选项； b) 评估该措施的有效性和周期性
	选择适当的信息安全风险处置选项[GB/T 22080—2016 的 6.1.3 a)]
	审核员宜确认有关风险处置过程的文件化信息，包含组织用于选择适当信息安全风险处置选项的方法的描述。审核员还宜确认此描述与组织实际执行的内容相对应。 请注意，GB/T 29246—2017 中 2.79 的注 1 列举了七种风险处置选项，并且在 GB/T 22080—2016 的 6.1.3 中引用了 ISO 31000:2009 的注释。 审核员宜验证风险准则与风险处置计划之间的一致性。组织宜能解释它在风险处置选项方面做出的决策，即使它们没有被记录。 审核员宜审核组织选定的风险处置选项。审核员还宜评审所选风险处置选项的适当性。 审核员宜验证最近的变更（例如新的 IT 系统或业务过程）是否已适当纳入风险评估和风险处置决策
	确定所有必要的控制[GB/T 22080—2016 的 6.1.3 b)]
	审核员宜确认有关风险处置过程的文件化信息，包含组织用于确定必要信息安全控制的方法的描述。审核员还宜确认此描述符合组织实际执行的操作。 [GB/T 22080—2016 的 6.1.3 d]要求适用性声明包含必要的控制以及附录 A 中包含但不必要的控制。它们可能是特定部门的控制（作为行业特定标准，例如 ISO/IEC 27011、ISO/IEC 27017）。他们也可能是“定制化控制”，因为组织可自己设计或从任何来源识别[见 GB/T 22080—2016 的 6.1.3 b)]。 确定实现风险处置选项的所有控制都宜包含在适用性声明中。此外，任何定制化控制宜在要求和实现中明确定义
	与附录 A [GB/T 22080—2016 的 6.1.3 c)] 进行比较
	通过评审适用性声明来证明符合此要求
	制定适用性声明[GB/T 22080—2016 的 6.1.3 d)]
	审核员宜验证适用性声明是否包含： a) 应用 GB/T 22080—2016 过程所确定的必要控制 6.1.3 的 b)和 c)； b) 包含它们的理由（例如，参考使用它的风险处置选项）； c) 是否实现了必要的控制； d) 所有被删减的附录 A 的控制的理由，例如： 1) 控制适用于组织不涉及的活动； 2) 组织使用定制化控制，不需附录 A 的控制； 3) 组织使用定制化控制，其作用与附录 A 控制相同（更多信息见 GB/T 31496—2015）； e) 相关的行业特定控制，这些控制将被指定为必要的控制，或以附录 A 删减的控制相同的方式进行处置。 因此，审核员宜确认实现选定风险处置选项所需的控制与适用性声明之间的一致性

表 A.2（续）

审核实践指南	**制定风险处置计划[GB/T 22080—2016 的 6.1.3 e)]**
	审核员宜确认有关风险处置过程的文件化信息，包含组织用于制定风险处置计划的方法描述。 审核员还宜确认风险处置计划是根据 GB/T 22080—2016 的 6.1.3 a)～c)制定的。 审核员宜进一步确认处置计划中提供的信息包括： a) 计划所涉及的风险； b) 必要的控制； c) 如何采取必要的控制来修改风险以便于满足风险接受准则； d) 风险责任人； 注 11：风险责任人负责批准风险处置计划并接受残余风险。 e) 选定的风险处置选项； f) 必要控制的实现状态； g) 选择处置选项的原因，包括可获得的预期收益； h) 处置计划包括的责任人、时间表和进度； i) 包括意外事件在内的资源需求； j) 绩效考核和约束； k) 报告和监视。 审核员宜评审风险处置计划是否考虑了组织的目标设定和管理过程，并与相关利益方进行了讨论
	获得风险责任人批准[GB/T 22080—2016 的 6.1.3 f)]
	审核员宜确认组织： a) 确定了风险责任人； b) 记录了残余风险； c) 获得风险责任人对信息安全风险处置计划的批准和对残余风险的接受
	文件化信息
	审核员宜确认有关风险处置的文件化信息真实存在。确保有关信息的文件化信息是合理的，安全风险处置过程含以下描述： a) 选择适当的信息安全风险处置选项的方法； b) 确定必要控制的方法； c) GB/T 22080—2016 附录 A 如何用于确定无意中忽略的必要控制； d) 如何编制 SOA； e) 如何编制风险处置计划； f) 如何获得风险责任人的批准。 注 12：对组织风险处置计划的内容或格式没有特别要求。
支持性文件	ISO 31000:2009 的 5.5、5.7 ISO/IEC 27003:2017 的 6.1.3、8.3 GB/T 25067—2020
A.3.2 信息安全目标及其实现规划(6.2)	
GB/T 22080—2016 中相关章条	5.1、5.2、7.1、7.3、7.4、7.5、9.1、9.3、10.2
GB/T 29246 中相关定义	信息安全、目标

表 A.2（续）

审核证据	审核证据可通过与信息安全目标及其实现规划相关的文件化信息或其他信息获得
审核实践指南	需注意的是，信息安全目标及其实现规划(GB/T 22080—2016 的 6.2)与领导和承诺(5.1)、方针(5.2)存在关联。 审核员宜确认： a) 信息安全目标是在组织相关职能和层面上建立的； b) 信息安全目标以其实现可进行检测的方式进行详细说明； c) 必要时(可能存在信息安全目标无法进行测量的情况)，目标可测量； d) 根据监视、测量、分析和评价(9.1)的要求，定期核实信息安全目标及其实现规划的现状和进展，并酌情进行更新，与持续改进的要求保持一致； e) 信息安全目标及其实现规划根据沟通(7.4)要求进行沟通； f) 根据文件化信息(7.5)的要求创建并控制目标的文件化信息。 审核员还宜验证： a) 实现信息安全目标(即“什么”)和相关时间范围(即“何时”)所需的措施得以确定； b) 责任分配(即“谁”)根据组织的角色、责任和权限(5.3)的要求得以建立； c) 适用的信息安全要求、风险评估和风险处置结果在目标及其实现规划中予以考虑； d) 任何实现目标的需求(例如预算、专业技能、技术或基础设施等)根据资源(7.1)要求得以确定并提供； e) 用于评价完成事项总体结果的机制根据监视、测量、分析和评价(9.1)的要求得以确定，并根据管理评审(9.3)的要求进行报告
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO/IEC 27003:2017 的 6.2
A.4 支持(7)	
A.4.1 资源(7.1)	
GB/T 22080—2016 中相关章条	5.1、6.2、7.2
GB/T 29246 中相关定义	持续改进、管理制度
审核证据	审核证据可通过文件化信息或组织所需资源的其他信息获得： a) 建立并实施 ISMS(包括其运行与控制)； b) 持续改进 ISMS。 资源包括： a) 人员； b) 专业技能或知识； c) 组织的基础设施(例如建筑物、通信线路等)； d) 技术； e) 信息以及与信息和信息处置相关的其他资产设备； f) 资金(例如现金、流动证券和信贷额度)
审核实践指南	审核员宜确认组织计划、确定和分配了建立和实施 ISMS 所需的资源(包括其运行与控制)，以及维护和持续改进所需的资源
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000:2009 的 4.3.5

表 A.2（续）

A.4.2 能力（7.2）	
GB/T 22080—2016 中相关章条	5.3、7.1、7.5.1 注、9.1 d)和 9.1 e)、9.2 e)
GB/T 29246 中相关定义	能力、有效性
审核证据	审核证据可通过文件化信息或其他相关信息获得： a) 组织的角色、责任和权限； b) 岗位描述； c) 所需的能力； d) 教育记录； e) 培训计划、课程和教育活动； f) 保留适当的文件化信息作为能力的证据； g) 评估其有效性。 GB/T 22080—2016 的 7.2 将能力范围扩至非组织成员。该要求规定他们“在组织的控制下工作”。示例可包括分包商和志愿者。 第三方要求的审核证据宜限于证明为 ISMS 组织执行的职能和活动
审核实践指南	审核员宜确认组织： a) 确定： 1) 组织控制下从事会影响组织信息安全绩效的工作人员； 2) 人员获得预期结果的知识和技能； 3) 人员运用知识和技能达到预期结果的能力。 b) 确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作。 c) 适用时，采取措施以获得必要的能力，并评估所采取措施的有效性
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 GB/T 31496—2015 的 7.2 ISO/IEC 27021：2017 的附录 A
A.4.3 意识（7.3）	
GB/T 22080—2016 中相关章条	5.1 d)、5.2、9.1、9.2、10.1、10.2
GB/T 29246 中相关定义	符合性、有效性、绩效、策略
审核证据	审核证据可通过以下方面的文件化信息或其他信息获得： a) 信息安全方针； b) 信息安全目标； c) 信息安全绩效； d) 不符合的纠正措施； e) 组织的角色、责任和权限； f) 岗位描述； g) 适用的学习计划和培训材料
审核实践指南	审核员宜确认在组织的控制下，工作人员能意识到： a) 信息安全方针； b) 其对 ISMS 有效性的贡献，包括改进信息安全绩效带来的益处； c) 不符合 ISMS 要求带来的影响。 审核员宜访谈适当数量的人员作为抽样，以确认他们了解这些信息。 对方针的认识不宜被视为需记住方针；相反，人们宜认识到关键的方针承诺及其在实现这些承诺方面的作用。 审核员还可在非专门用于信息安全的意识和培训计划中找到信息安全意识证据。这些活动可与最高管理者的沟通活动密切相关［GB/T 22080—2016 的 5.1 d)和 7.4］

表 A.2（续）

支持性文件	ISO/IEC 导则第 1 部分:2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO/IEC 27003:2017 的 7.3
A.4.4 沟通（7.4）	
GB/T 22080—2016 中相关章条	5.1、5.2、5.3、6.2、9.2
GB/T 29246 中相关定义	方针
审核证据	审核证据可通过文件化信息或其他信息获得： a） 信息安全方针； b） 组织的角色、责任和权限； c） 信息安全风险评估过程； d） 信息安全风险处置过程； e） 信息安全目标； f） 过程已按计划执行的信息； g） 信息安全风险评估结果； h） 信息安全风险处置结果； i） ISMS 绩效； j） 审核结果； k） 管理评审结果
审核实践指南	审核员宜确认组织的沟通需求已根据 GB/T 22080—2016 的沟通要求得到有效的识别、实现和维护。 证据的示例可包括： a） 会议记录中的信息； b） 正式的沟通计划、文件化规程和结果； c） 与分配到特定角色的人员进行面谈，以证明他们知悉与其角色相关的沟通要求：沟通什么、何时沟通、与谁沟通、谁来沟通以及影响沟通的过程。 这些证据可补充： a） 下列沟通信息： 1） 有效的信息安全管理的重要性以及 ISMS 要求的符合性； 2） 方针； 3） 责任和权限； 4） ISMS 绩效； 5） 目标； 6） 对 ISMS 有效性的贡献，包括改进信息安全绩效带来的益处； 7） 不符合 ISMS 要求带来的影响； 8） 审核结果。 b） 正式的沟通计划、文件化规程和结果。 审核员宜验证组织是否已确定其与 ISMS 相关的沟通需求，例如，这些需求可包括透明度、适当性、可信度、回应性、清晰度以及保护。 沟通可是口头或书面、单向或双向、内部或外部的
支持性文件	ISO/IEC 导则第 1 部分:2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000:2009 的 4.3.6、4.3.7 ISO/IEC 27003:2017 的 7.4

表 A.2（续）

A.4.5 文件化信息（7.5）	
A.4.5.1 总则（7.5.1）	
GB/T 22080—2016 中相关章条	4.3、5.2 e)、6.1.2、6.1.3、6.2、7.2 d)、8.1、8.2、8.3、9.1、9.2 g)、9.3 和 10.1
GB/T 29246 中相关定义	文件化信息
审核证据	审核证据可通过 ISMS 中的文件化信息或其他信息进行创建、控制或维护，包括： a) 管理体系的范围； b) 方针； c) 目标； d) 能力的证据； e) 管理体系运行规划和控制所需的外部信息； f) 信息安全风险评估过程； g) 信息安全风险处置过程； h) 适用性声明； i) 必要的信息，以确保过程和确定的控制按计划进行； j) 信息安全风险评估结果； k) 信息安全风险处置结果； l) 监视、测量、分析和评估结果； m) 内部审核计划及其实施的证据； n) 内部审核结果； o) 管理评审结果； p) 不符合的原因和采取的措施； q) 纠正措施结果。 文件化信息是为需求而创建，并非为满足 GB/T 22080—2016 的要求而创建
审核实践指南	审核员宜确认该组织的 ISMS 包括： a) GB/T 22080—2016 要求的文件化信息； b) 组织确定必要的 ISMS 体系有效性的文件化信息。 叙述“文件化信息作为……的证据”意味着之前的术语“记录”。 审核员宜确认组织确定除了 GB/T 22080—2016 明确要求的 ISMS 的有效性之外，还需哪些文件化信息，这些因素宜在审核证据列表中被考虑。 术语“文件化信息”是指 GB/T 22080—2016 确定的信息，可以任何格式或介质来控制和维护（见 7.5.3）。 审核员宜按照 7.5.2 和 7.5.3 的要求确认创建和控制文件化信息
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000：2009 的 5.7 ISO/IEC 27003：2017 的 7.5.1
A.4.5.2 创建和更新（7.5.2）	
GB/T 22080—2016 中相关章条	4.3、5.2 e)、6.1.2、6.1.3、6.2、7.2 d)、8.1、8.2、8.3、9.1、9.2 g)、9.3 和 10.1
GB/T 29246 中相关定义	文件化信息

表 A.2（续）

审核证据	审核证据可通过以下方面的文件化信息或其他信息获得： a） 允许明确和具有唯一标识的共同属性； b） 使用的格式和介质； c） 上次评审或更新的日期； d） 变更的历史； e） 评审者和批准者的身份
审核实践指南	审核员宜确认在创建和更新文件化信息时，组织确保适当： a） 标识和描述（例如标题、日期、作者或引用编号）； b） 格式（例如语言、软件版本、图表）和介质（例如纸质的、电子的）； c） 对适宜性和充分性的评审和批准。 注 13：用于文件化信息的标识、格式和介质是组织实施 GB/T 22080—2016 的选择；它不必是文本格式或纸质手册的形式。 如若 ISMS 范围内的文件化信息提交审核，审核员宜抓住机会执行这些审核任务。它们不必每次都进行，只需达到足够次数即可确认符合 GB/T 22080—2016 的 7.5.2 相关要求
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO/IEC 27003:2017 的 7.5.2
A.4.5.3 文件化信息的控制（7.5.3）	
GB/T 22080—2016 中相关章条	4.3、5.2 e）、6.1.2、6.1.3、6.2、7.2 d）、8.1、8.2、8.3、9.1、9.2 g）、9.3 和 10.1
GB/T 29246 中相关定义	文件化信息
审核证据	审核证据可通过以下活动的文件化信息或其他信息获得： a） 分发、访问、检索和使用； b） 存储和保护，包括保持可读性； c） 控制变更（例如版本控制）； d） 保留和处置； e） 文件化信息库的结构和配置
审核实践指南	审核员宜确认 ISMS 和 GB/T 22080—2016 要求的文件化信息得以控制，以确保： a） 无论何时何地，必要时是可用且适用的； b） 受到充分保护（例如，保密性、不当使用或完整性丧失）。 审核员宜确认组织适用时处理了以下问题： a） 分发、访问、检索和使用； b） 存储和保存，包括保持可读性（以数字或其他格式或手写）； c） 控制变更（例如版本控制）； d） 保留和处置。 如若 ISMS 范围内的文件化信息提交审核，审核员宜抓住机会执行这些审核任务。它们不必每次都进行，只需达到足够次数即可确认符合 GB/T 22080—2016 的 7.5.3 相关要求

表 A.2（续）

支持性文件	ISO/IEC 导则第 1 部分:2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000:2009 的 5.7 ISO/IEC 27003:2017 的 7.5.3
A.5 运行（8）	
A.5.1 运行规划和控制(8.1)	
GB/T 22080—2016 中相关章条	4.4、6.1.1、6.1.2、6.1.3、6.2、7.5.1、9.1 和 9.2
GB/T 29246 中相关定义	后果、信息安全、目标、组织、外包、处理、要求
审核证据	审核证据可通过文件化信息或其他信息获得： a) 组织需确认运行控制处理已按照计划得到实施(GB/T 22080—2016 的 8.1)； b) 组织有必要确认 ISMS 的有效性 [GB/T 22080—2016 的 7.5.1 b)]； c) ISMS 规划（GB/T 22080—2016 的 6.1.1)； d) 信息安全目标（GB/T 22080—2016 的 6.2）
审核实践指南	审核员宜确认组织规划、实现和控制满足组织运行中信息安全要求所需的过程，以确保完成 GB/T 22080—2016 中的要求，并确定风险优先级以及其他因素。 审核员宜确认运行控制包括实施的方法和信息安全控制，确保业务操作、活动或设备符合规定的条件、绩效标准或遵从法规的限制，从而有效地实现 ISMS 的预期结果。这些控制的建立实现了业务过程需要的最佳功能所必需的技术要求，例如技术规范或操作参数或特定的方法。 宜对与业务过程相关的运行控制和信息安全控制的情况进行评审，在这些业务过程中，缺少运行控制和信息安全控制可能导致偏离方针和目标或构成不可接受的风险。这些情况可能与业务操作、活动、过程、生产、安装、服务、维护、合同方、供应商或外包商有关。所执行的控制程度将取决于许多因素，包括所执行的功能、它们的重要性或复杂性、偏离的潜在后果、可变性或所涉及的可用的技术能力。 因此，审核员宜审核组织： a) 实施在“应对风险和机会的措施”中所确定的活动(GB/T 22080—2016 的 6.1)； b) 执行计划以实现已确定的信息安全目标，并制定计划实现这些目标(GB/T 22080—2016 的 6.2)； c) 创建和控制所需的文件，以确认运行控制和信息安全控制已按照文件化信息的要求按计划进行(GB/T 22080—2016 的 7.5)； d) 控制计划的变更并审核意外变更的后果，以防止或以最大限度地减少未满足技术要求或引入新风险的可能性； e) 当运行控制失败时，采取必要的措施来解决任何由此产生的不良影响； f) 确保外包过程是确定和受控的，例如：将运行控制应用限制为局部控制或影响的程度，并且将不会在外包处置过程中改变与外部实体的法律关系
支持性文件	ISO/IEC 导则第 1 部分:2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO/IEC 27003:2017 的 8.1
A.5.2 信息安全风险评估（8.2）	
GB/T 22080—2016 中相关章条	6.1.2
GB/T 29246 中相关定义	信息安全

表 A.2（续）

审核证据	审核证据可通过文件化信息或其他有关信息获得： a) ISMS 规划(GB/T 22080—2016 的 6.1.1)； b) 信息安全风险评估过程(GB/T 22080—2016 的 6.1.2)； c) 信息安全风险评估结果(GB/T 22080—2016 的 8.2)； d) 适用性声明； e) 风险处置计划
审核实践指南	审核员宜确认(GB/T 22080—2016 的 6.1)定义和应用的信息安全风险评估过程得以实施并已纳入组织运行中，按计划的时间间隔或当重大变更提出或发生时执行信息安全风险评估，同时考虑了 GB/T 22080—2016 的 6.1.2 a)中已建立的准则。 审核员宜评估： a) 风险评估的计划周期同样适合于 ISMS； b) 当 ISMS(或其环境)发生任何重大变更或发生信息安全事件时，组织确定哪些变更或事件需要进行额外的信息安全风险评估以及如何触发这些评估。 有关其他信息，请参阅 A.3.1.2 的审核实践指南
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000：2009 的 5.4.1 ISO/IEC 27003：2017 的 8.2
A.5.3 信息安全风险处置（8.3）	
GB/T 22080—2016 中相关章条	6.1.3、附录 A
GB/T 29246 中相关定义	控制、控制目标、文件化信息、信息安全、残余风险、风险评估、风险准则、风险责任人、风险处置
审核证据	审核证据可通过文件化信息或其他有关信息获得： a) ISMS 规划； b) 信息安全风险处置过程； c) 风险处置计划； d) 信息安全风险处置结果； e) 适用性声明
审核实践指南	审核员宜确认在“ISMS 规划”(GB/T 22080—2016 的 6.1)中定义和应用的信息安全风险处置过程已实施并整合到组织运行中，并在每次信息安全风险评估（GB/T 22080—2016 的 8.2)迭代后或当风险处置的实施(部分)失败时得以执行。 有关其他信息，请参阅 A.3.1.3 的审核实践指南
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO 31000：2009 的 5.5 ISO/IEC 27003：2017 的 8.3
A.6 绩效评价(9)	
A.6.1 监视、测量、分析和评价(9.1)	
GB/T 22080—2016 中相关章条	5.3 b)、6.1.1 e)、6.2
GB/T 29246 中相关定义	持续改进、有效性、测量、监视、绩效、信息安全事态、信息安全事件、信息需求、测度

表 A.2（续）

审核证据	审核证据可通过文件化信息或关于监视、测量、分析和评价结果的其他信息获得（参见GB/T 22080—2016 的 9.1）。 证据也可通过文件化信息或其他有关的信息获得： a） 相关职能和层级的信息安全目标； b） 规划如何实现信息安全目标； c） 实现信息安全目标的情况和程度； d） 向最高管理者报告 ISMS 的执行情况［参见 GB/T 22080—2016 的 5.3 b）］； e） 风险评估结果及风险处置选项现状； f） 监视、测量、分析、评价方法； g） 内部审核方案和审核结果； h） 管理评审和管理评审结果； i） 信息安全事态报告（见 GB/T 22080—2016 的 A.16.1.2）； j） 信息安全漏洞报告（见 GB/T 22080—2016 的 A.16.1.3）； k） 信息安全事件报告（见 GB/T 22080—2016 的 A.16.1.4）
审核实践指南	审核员宜确认组织： a） 评估 ISMS 的信息安全绩效和有效性； b） 已确定： 1） 需要被监视和测量的内容，包括信息安全过程和控制； 2） 适用时，监视、测量、分析和评价的方法，以确保得到有效的结果； 3） 何时宜执行监视和测量； 4） 谁宜监视和测量； 5） 何时宜分析和评价监视和测量的结果； 6） 谁宜分析和评价这些结果。 审核员宜使用文件化信息作为证据来评审信息安全绩效，例如计划、对最高管理者提交的 ISMS 绩效报告、管理评审结果、内部审核报告和信息安全事态、弱点事件报告。 审核员宜评估不符合、处置失误、信息安全漏洞和其他事件的预测、检测、报告和处理的程度。审核员宜确定组织是否以及如何评估应对风险和机会的措施的有效性，以确保在风险处置中信息安全控制得到有效实现和运行。 审核员还宜评估对信息安全绩效的执行情况，以促进 ISMS 的持续改进。审核员还宜确认，变更将作为反映风险评估和风险处置过程的结果（GB/T 22080—2016 的 8.1 和 8.2）。此外，审核员宜确认应对风险和机会的措施的文件化信息已更新。 审核员宜审核被监视或测量、分析和评价的特征信息是必要的，并且充分地判断这些 ISMS 计划措施的实现程度和成果。审核员宜确认通过监视或测量、分析和评价获得的信息是按照管理评审的要求提交给最高管理者的（GB/T 22080—2016 的 9.3）。 注 14：如果一个组织遵循 GB/T 31497 中的指导，除了“信息需求”之外，它还可使用术语“绩效测度”和“有效性测度”。
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9
A.6.2 内部审核（9.2）	
GB/T 22080—2016 中相关章条	9.3
GB/T 29246 中相关定义	审核、审核范围、能力

表 A.2（续）

审核证据	审核证据可通过文件化信息或其他有关信息获得： a） 内部审核方案； b） 内部审核计划； c） 内部审核结果； d） 内部审核员的权限； e） 管理评审结果
审核实践指南	注 15：A.6.2 为外部审核、自我检查或同行评估提供相关内部审核指导。 审核员宜确认组织规划、实现和维护一个内部审核方案，以便提供关于 ISMS 是否符合 GB/T 22080—2016 要求和组织自己附加的任何 ISMS 相关要求的信息，以及 ISMS 是否按计划有效实施和维护。 审核员宜验证内部审核方案： a） 内部审核是根据相关过程的重要性和以往审核的结果来计划和安排的； b） 制定和实施内部审核的方法； c） 考虑到内部审核过程的完整性和独立性，分配审核方案内的职责和分工； d） 定义每次审核的审核准则和范围； e） 设计目的是提供 ISMS 是否符合下列要求的信息： 1） GB/T 22080—2016 的要求； 2） 组织自身要求； f） 旨在提供信息以确认 ISMS 是否得到有效实现和维护。 审核准则示例：对可核实的记录、事实陈述或其他信息（例如政策、规程和要求）进行比较，审核范围可包括物理位置、组织单位、活动和过程的描述，以及相关审核所涵盖的时间段。 审核员宜确认内部审核方案和审核是由内部人员计划、实现和维护，或由代表组织行事的外部人员进行管理。在任何一种情况下，审核员宜确认负责管理内部审核方案的人员和执行内部审核的审核员是否可满足能力（参见 GB/T 22080—2016 的 7.2 和 9.2）要求和指南（参见 GB/T 22080—2016 的 7.2）。 审核员宜确认内部审核结果向负责审核的职能部门/单位的管理层以及满足相关沟通（GB/T 22080—2016 的 7.4）要求的任何其他人员进行报告。审核员宜确认内部审核结果的信息，包括趋势，是否按照管理评审（参见 GB/T 22080—2016 的 9.3）的要求进行了评审
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 本标准 GB/Z 32916 GB/T 27021.1—2017 的 9.3.1.2.2 g）、9.3.1.3 e）、9.4.8.3 a）、9.6.2.2 a） GB/T 25067—2020 的 9.1.5.1、9.3.1.2.2 h）、9.5.1、9.6.2.1.1 a）
A.6.3 管理评审（9.3）	
GB/T 22080—2016 中相关章条	4.1、4.2、8.2、8.3、9.1、9.2、10.1 和 10.2
GB/T 29246 中相关定义	持续改进、有效性、绩效

表 A.2（续）

审核证据	审核证据可通过文件化信息或其他有关信息获得： a) 按计划的时间间隔进行评审； b) 以往管理评审的措施状况； c) 与 ISMS 相关的外部和内部事项的变更； d) 对信息安全绩效的反馈，包括不符合和纠正措施、监视和测量结果、审核结果和信息安全目标完成的情况等趋势； e) 相关方的反馈； f) 风险评估结果及风险处置计划的状态； g) 持续改进的机会
审核实践指南	审核员宜确认，最高管理者已按计划的评审时间表进行管理评审，评审输入的所有信息，并提供预期的输出。 审核员宜通过审核来评估最高管理者是否亲自参与评审，实施该机制以推动 ISMS 的更新，并指导持续改进措施的优先顺序，特别是与组织背景不断变化的事项有关的预期的结果或有利的条件和结果。 审核员宜验证管理评审是否包括对 A.6.3 审核证据所列的 b)～g)所有项目的考虑。 审核员还宜确认，管理评审的输出结果包括 ISMS 变更的持续改进机会和任何需求相关的决策
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9 ISO/IEC 27003:2017 的 9.3
A.7 改进(10)	
A.7.1 不符合及纠正措施(10.1)	
GB/T 22080—2016 中相关章条	7.5、8.1、10.2
GB/T 29246 中相关定义	纠正、纠正措施、有效性、不符合
审核证据	审核证据可通过文件化信息或其他有关信息获得： a) 不符合的性质及所采取的任何后续措施； b) 任何纠正措施的结果； c) 监视和测量的结果； d) 审核计划和审核结果； e) 管理评审结果； f) 与信息安全有关的相关方的要求； g) 纠正措施带来的 ISMS 变更
审核实践指南	审核员需确认： a) 当不满足 GB/T 22080—2016 和 ISMS(包括运行)要求时，组织通过发现不符合并要求采取纠正措施来做出响应； b) 不符合和纠正措施包括采取措施纠正现状、检查不符合的原因并确定其他地方是否发生或将潜在发生，以确保措施可用于预防不符合再次发生； c) 组织的响应包括对确认达到预期结果而采取的措施的评价，以及对 ISMS 的评价以确定是否需要变更以避免将来发生类似的不符合； d) 不符合、纠正措施及结果的文件化是根据文件化信息的要求创建和控制的(见 GB/T 22080—2016 的 7.5)
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9

表 A.2（续）

A.7.2 持续改进（10.2）	
GB/T 22080—2016 中相关章条	5.1、5.2、6.1、6.2、7.1、8.1、9.1、9.2、9.3、10.1
GB/T 29246 中相关定义	持续改进、有效性、绩效
审核证据	审核证据可通过文件化信息或其他有关信息获得： a） 不符合的性质以及随后采取的任何措施，包括报告纠正措施； b） 任何纠正措施的结果； c） 监视和测量结果； d） 审核计划和审核结果； e） 管理评审结果； f） 与信息安全有关的相关方的要求； g） 对信息安全事件的评估和决策（参见 GB/T 22080—2016 的 A.16.1.4）
审核实践指南	审核员宜确认组织将开展循环的活动，以提高 ISMS 适宜性、充分性和有效性。 审核员宜评审并验证持续改进是否涉及对 ISMS 的设计和实现进行更改，以提高组织符合 ISMS 要求并实现其目标和方针承诺的能力。 审核员宜通过审核确认组织： a） 开展实现改进的活动，包括但不限于： 1） 采取措施应对风险和机会（参见 GB/T 22080—2016 的 6.1）； 2） 制定目标（参见 GB/T 22080—2016 的 6.2）； 3） 提升运行控制（参见 GB/T 22080—2016 的 8.1），考虑新技术、新方法或新信息； 4） 绩效分析与评价（参见 GB/T 22080—2016 的 9.1）； b） 实施内部审核（参见 GB/T 22080—2016 的 9.2）； c） 实施管理评审（参见 GB/T 22080—2016 的 9.3）； d） 检测不符合并实施纠正措施（参见 GB/T 22080—2016 的 10.1）； e） 根据监视、测量、分析和评价（GB/T 22080—2016 的 9.1）、内部审核（GB/T 22080—2016 的 9.2）和管理评审（GB/T 22080—2016 的 9.3）的要求，定期评价和评审 ISMS，以确定改进的机会，并根据应对风险和机会的措施（GB/T 22080—2016 的 6.1）、目标及其实现规划（GB/T 22080—2016 的 6.2）以及运行规划和控制（GB/T 22080—2016 的 8.1）等规划适当的措施
支持性文件	ISO/IEC 导则第 1 部分：2017 年融合的 JTC1 补充部分中附录 JC 的 JC.9

参 考 文 献

[1] GB/T 22081 信息技术 安全技术 信息安全控制实践指南(GB/T 22081—2016,ISO/IEC 27002:2013,IDT)

[2] GB/T 25067—2020 信息技术 安全技术 信息安全管理体系审核和认证机构要求(ISO/IEC 27006:2015,IDT)

[3] GB/T 27021.1—2017 合格评定 管理体系审核认证机构要求 第1部分:要求(ISO/IEC 17021-1:2015,IDT)

[4] GB/T 27024 合格评定 人员认证机构通用要求(GB/T 27024—2014,ISO/IEC 17024:2012,IDT)

[5] GB/T 31496—2015 信息技术 安全技术 信息安全管理体系实施指南(ISO/IEC 27003:2010,IDT)

[6] GB/T 31497 信息技术 安全技术 信息安全管理 测量(GB/T 31497—2015,ISO/IEC 27004:2009,IDT)

[7] GB/T 31722 信息技术 安全技术 信息安全风险管理(GB/T 31722—2015,ISO/IEC 27005:2008,IDT)

[8] GB/Z 32916 信息技术 安全技术 信息安全控制措施审核员指南(GB/Z 32916—2016,ISO/IEC TR 27008:2011,IDT)

[9] ISO/IEC 27003: 2017 Information technology—Security Techniques—Information security management systems—Guidance

[10] ISO/IEC 27011 Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

[11] ISO/IEC 27017 Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[12] ISO/IEC 27021: 2017 Information technology—Security Techniques—Competence requirements for information security management systems professionals

[13] ISO 31000:2009 Risk management—Principles and guidelines

[14] ISO/IEC Directives Part 1 Consolidated JTC1 Supplement 2017—Procedures specific to JTC1

[15] IAF MD1.2007 IAF Mandatory Document for the Certification of Multiple Sites Based on Sampling, International Accreditation Forum