安全加社区

公益译文项目

2020

评估信息安全持续监控（ISCM）项目：

ISCM 项目评估方法

美国国家标准与技术研究院（NIST）

2020 年 5 月

文档信息			
原文名称	Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment		
原文作者	Kelley Dempsey, Victoria Yan Pillitteri, Chad Baer, Robert Niemeyer, Ron Rudman, Susan Urban	原文发布日期	2020 年 5 月
原文发布单位	美国国家标准与技术研究院（NIST）		
原文出处	https://doi.org/10.6028/NIST.SP.800-137A		
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

免责声明

• 本文原文来自于互联网的公共方式，由“安全加”社区出于学习交流的目的进行翻译，而无任何商业利益的考虑和利用，“安全加”社区已经尽可能地对作者和来源进行了通告，但不保证能够穷尽，如您主张相关权利，请及时与“安全加”社区联系。

•“安全加”社区不对翻译版本的准确性、可靠性作任何保证，也不为由翻译不准确所导致的直接或间接损失承担责任。在使用翻译版本中所包含的技术信息时，用户同意“安全加”社区对可能出现的翻译不完整、或不准确导致的全部或部分损失不承担任何责任。用户亦保证不用做商业用途，也不以任何方式修改本译文，基于上述问题产生侵权行为的，法律责任由用户自负。

计算机系统技术报告

美国国家标准与技术研究院（NIST）信息技术实验室（ITL）为美国的测量和标准基础设施提供技术领导，促进美国的经济与公共福利。ITL 负责开发测试，制定测试方法，并提供参考数据、概念验证实现和技术分析来推动信息技术的发展和生产应用。ITL 的职责包括制定管理、行政、技术及物理方面的标准和指南，实现经济高效的安全，并保护联邦信息系统中非国家安全相关信息的隐私。特别刊物（SP）800 系列文件聚焦于 ITL 在信息系统安全方面的研究、指导和外展活动以及联合业界、政府和各学术机构开展的协作活动。

摘要

本文介绍了信息安全持续监控（ISCM）项目的评估方法，联邦、州和地方政府组织和商业企业可使用该方法评估自己的 ISCM 项目。ISCM 项目评估包括对 ISCM 战略、政策、程序、运营和持续监控数据分析的审核。通过评估，组织领导可了解本组织 ISCM 项目的有效性和全面性。各组织可直接使用本文提供的 ISCM 评估方法，也可以基于该方法开发适合本组织的评估方法。本文还提供了评估原则和评估程序示例，方便组织使用。

关键词

评估；评估要素；评估方法；评估程序；持续监控；信息安全持续监控；ISCM 项目；ISCM 项目评估

执行摘要

为了有效地管理网络安全风险，组织需持续了解自己的信息安全状况、漏洞和威胁[1]。要获取这种信息以及更有效地管理风险，组织可以 ISCM 项目为指导，实现信息安全持续监控（ISCM）能力。ISCM 项目对 ISCM 进行定义，组建相关团队，全面实施并运营 ISCM，为组织提供必要信息，促使组织各风险管理级别（组织级、任务/业务流程级和系统级）就安全状况做出基于风险的决策。

组织需要一种方法来确定和评估已建立的 ISCM 项目是否根据风险有效地管理了组织的安全状况。本文基于各种评估标准（包括 NIST SP 800-137《联邦信息系统和组织的信息安全持续监控》（ISCM）；SP 800-37《信息系统与组织的风险管理框架：安全与隐私的生命周期方法》》；SP 800-39《管理信息安全风险：组织、任务与信息系统视角》；行政管理和预算局（OMB）的通知及备忘录），提出了 ISCM 项目评估方法。根据本指南开发的 ISCM 项目评估方案，针对的是 ISCM 项目本身（即 ISCM 项目的结构和治理），而不是 ISCM 项目的实施结果或所使用的持续监控技术。有效的 ISCM 项目评估方案输出的结果是一致的，不受评估实体的影响。本文并未要求在评估 ISCM 项目时评估单个控制措施或检视控制措施的评估结果。

ISCM 项目评估的首要目标是为组织提供 ISCM 项目改进建议，从而管理和降低组织所面临的风险。ISCM 项目评估方法可用于评估组织的 ISCM 战略、政策、程序、实施、操作步骤、分析过程、具体报告、结果展示、风险评估和风险评分、风险响应以及 ISCM 项目改进流程。ISCM 项目评估方案可由组织针对自己的 ISCM 项目自行制定，也可由独立的评估机构制定。

开发或采用、实施 ISCM 项目评估方案可发现 ISCM 项目、ISCM 项目实施或 ISCM 结果应用中的差距，帮助组织降低总体风险。此外，通过 ISCM 项目评估，可了解各系统的持续授权是否已准备就绪。

本文档：

- 为组织各风险管理级别（定义见 NIST SP 800-39《管理信息安全风险：组织、任务与信息系统视角》）开展 ISCM 项目评估提供指导；
- 阐述了 ISCM 项目评估与重要安全概念和过程的相关性，如 NIST 风险管理框架（RMF）、全组织风险管理级别、组织治理、ISCM 指标和持续授权；
- 介绍了有效的 ISCM 项目评估所具备的特点；
- 提出了 ISCM 项目评估标准（同时提供了参考来源），组织可采用这些标准进行 ISCM 项目评估，或基于这些标准制定适合本组织的评估标准；
- 介绍了通过评估程序进行 ISCM 项目评估的方法，该评估程序在相关配套文件（包含 ISCM 项目评估要素一览表）中进行了定义，用以开发可复用的评估流程。

[1] NIST SP 800-137《联邦信息系统和组织的信息安全持续监控（ISCM）》将 ISCM 定义为“实时了解信息安全、漏洞和威胁，以支持组织的风险管理决策”。【[SP800-137, B-6 页】

目录

1. 概述

根据《2014 年联邦信息现代化法案》（FISMA）【FISMA2014】和行政管理和预算局（OMB）的通知及备忘录[2]，联邦机构须对组织信息安全状况实施持续监控。全面的持续监控项目可作为风险管理和决策支持工具，在组织各级全面实施。组织级战略和业务目标为任务/业务级活动和用以支持持续监控的系统级功能和技术提供指导方向。

NIST SP 800-137《联邦信息系统和组织的信息安全持续监控（ISCM）》【SP800-137】将信息安全持续监控定义为"实时了解信息安全、漏洞和威胁，以支持组织的风险管理决策"。ISCM 项目对 ISCM 进行定义，组建相关团队，实施并全方位运营 ISCM，为组织提供必要信息，促使组织各风险管理级别就安全状况做出基于风险的决策。

为有效应对日益增长的安全挑战，ISCM 项目应：

- 评估控制措施的有效性，监控安全状况[3]；
- 通过实施稳健的全组织持续监控流程，推广近乎实时的风险管理和持续系统授权概念；
- 结合流程，根据调查结果和组织的风险承受能力采取应对行动，保证该等行动达到预期效果。

本文（NIST SP 800-137A）为组织评估 ISCM 项目的完整性和有效性以及发现 ISCM 项目中的缺陷提供了指导。ISCM 项目评估方案旨在为组织提供 ISCM 项目要素评估方法，包括评审 ISCM 战略、政策、程序、实施规划、ISCM 指标、分析过程、具体结果展示/报告、风险应对和 ISCM 改进流程。本文使用的方法基于 SP800-137 提出的概念和原则以及为联邦组织制定的 ISCM 要求。

"评估"一词在本文中有两种含义，一种指需完成的 ISCM 项目评估活动，另一种指可复用的评估工具（如模板或空白工作表），具体含义可通过上下文判断。

1.1 背景

及时获取全面的安全信息，以便基于风险做出决策，这对组织来说是个长期存在的挑战，而 ISCM 项目正是为了解决这个挑战。有效的 ISCM 项目能够及时输出与安全相关的准确、完备信息，提交给组织的各级别决策者。组织级决策者可能不太清楚 ISCM 项目融入全组织风险管理战略的方式或原因，也不清楚该项目应属于风险管理的哪个环节。对于组织领导来说，重要的是理解业务需求和能力对 ISCM 项目的驱动作用。许多情况下，组织内部或已具备组织持续监控所需的能力。然而，若缺乏全面的战略将监控功能固化为 ISCM 功能，就无法真正实现 ISCM。

组织需要一个方法来评估为实施 ISCM 而规划、开发或获取的内容，内部开发的 ISCM 项目尤其需要这样一个方法。有了方法，组织才能判断 ISCM 项目是否妥善实施以及投资是否产生了回报。

要确定组织的 ISCM 项目是否有效，需要制定并实施规范的评估方案，让领导了解 ISCM 项目对预期目标的实现程度。ISCM 项目评估可围绕 ISCM 各方面的能力，提供相应的评估标准、判断和评分，还可以通过分析所收集的数据形成结论。

[2] 主要是 OMB 通知 A-130 (2016) [OMB A-130]和 OMB 备忘录 M-11-33[OMB M-11-33] 。OMB M-11-33 要求定期审查 ISCM 项目，确保持续监控妥善实施，足以支持基于风险的决策。OMB 通知 A-130 重申并固化了上述备忘录要求。

[3] 安全状况监控是对组织定义的组织安全状况衡量指标进行监控。

ISCM 项目评估还可以根据评估结果为组织提供建议。

网络安全与基础设施安全局（CISA）[4]与 NIST 的国家网络安全卓越中心（NCCoE）[5]合作，以 NIST 计算机安全部（CSD）发布的 SP800-137 为主要依据，发起并启动开发 ISCM 项目评估流程。

该评估流程（更多详细信息，参见即将发布的 NIST 跨部门或内部报告（NISTIR）8212【NISTIR8212】）是为 CISA 和联邦机构使用而开发的。ISCM 项目评估流程可适当调整，供联邦机构、商业组织和非联邦政府组织使用。组织可以以 NISTIR8212 为指南，作为对 NIST SP 800-137A 的补充，选择采用相同的方法来评估 ISCM 计划和方案。

1.2 目的

本文档：

- 为各组织风险管理级别开展 ISCM 项目评估提供指导；
- 定义了 ISCM 项目评估方法；
- 提出了详细的 ISCM 项目评估标准，供组织或评估结构使用；
- 介绍了有效的 ISCM 项目评估所具备的特点。

此外，可基于本指南编制 ISCM 项目评估方案，用以：

- 评估对现有 ISCM 项目所做的计划性修改；
- 为 ISCM 评估方案开发提供参考，进而为计划性或未来的 ISCM 项目指明方向；
- 监控 ISCM 项目评估中明确的国家或组织优先事项（例如内部威胁）或高优先级/可见性举措（例如高价值资产）的有效性。

1.3 读者对象

本文档的目标读者为持续监控信息安全态势和组织风险管理的个人，包括：

- 负责评审组织 ISCM 项目的个人，包括进行技术评审的管理人员和评估人员（如系统评估人、内部和第三方评估员/评估团队、独立验证/认证评估师、审计人员和系统负责人）；
- 承担任务/业务负责人或受托人责任的个人（如联邦机构负责人、首席执行官和首席财务官）；
- 需要考虑 ISCM 功能的系统开发/集成负责人（如项目经理、系统负责人、信息技术产品开发人员、系统开发人员、系统集成商、企业架构师、信息安全架构师和通用控件提供方）；
- 承担系统和/或安全管理/监督职责的个人（如高层领导人、风险管理人员、授权人、首席信息官、首席信息安全官[6]），这类人员需在一定程度上依赖于持续监控过程中输出的安全相关信息做出基于风险的决策；
- 负责系统和安全控制评估与监控的个人（如系统评估人、评估员/评估团队、独立验证/认证评估师、审计人员、系统负责人或系统安全主管）

[4] 有关 CISA 的更多信息，请访问 https://www.cisa.gov。
[5] 有关 NCCoE 的更多信息，请访问 https://nccoe.nist.gov。
[6] 在*联邦*组织层面，这一职位有时称为高级机构信息安全官（SAISO）。有些组织将此职位称为高级信息安全官（SISO），有些称为首席信息安全官（CISO）。

1.4 范围

本文档阐述了 ISCM 项目评估全过程，可用于评估跨组织 ISCM 项目的建立和运营。单个控制措施的评估和控制评估结果的检视不在 ISCM 项目评估的范围之内。

基于相关标准，可采用多种方法评估组织的项目或系统。本文档基于不同的评估标准，提出了一种评估方案开发方法。ISCM 项目评估针对的是 ISCM 项目的结构和治理，而非持续监控技术或技术实现。按本指南开发的评估方案具有技术中立性、灵活性和可扩展性，易于实施，适用于各种安全监控技术。各组织可基于本文所述方法，制定符合本组织特定需求的评估方案。

1.5 假设

本文假设读者熟悉 SP800-137 中提出的 ISCM 概念，并对 SP800-137 中定义和修订的 NIST 风险管理框架（RMF）有本职工作所需的必要了解，还假设读者熟悉 NIST SP 800-39【SP800-39】《管理信息安全风险：组织、任务与信息系统视角》中定义和修订的全组织风险管理流程和组织内部各风险管理级别。

1.6 内容简介

本文档其他章节内容如下：

- 第 2 章介绍了对组织风险管理中的 ISCM 进行评估的基本原则、ISCM 背景、与 NIST RMF 的交互、ISCM 项目评估标准及其来源、ISCM 项目评估标准的制定以及 ISCM 项目评估的实施，这些主题各自独立，相关性不大。
- 第 3 章阐述了 ISCM 项目的评估流程，包括评估的规划和执行、评估步骤和结果应用。第 3 章基于第 2 章中的内容，完整展示了 ISCM 项目的评估全过程。
- 参考资料部分列出了本文所参考的文献。
- 附录部分提供了 ISCM 的辅助信息，包括：（A）缩略词，（B）词汇表，和（C）评估要素关系图。
- 有一个单独的电子表格【一览表】提供了评估要素和评估程序的完整信息，用于构建 ISCM 项目评估要素。

2. 基本原则

本章解释了 ISCM 项目评估的基本原则。ISCM 项目评估是一个管理过程，用以检视以下各项的充分性和有效性：

- ISCM 战略规划；
- ISCM 项目的建立；
- ISCM 战略、政策、程序和指标的实施；
- ISCM 项目的运营；
- 对所收集数据进行的分析及结果报告；
- 对 ISCM 结果的响应；
- ISCM 流程改进

本章介绍的基本原则贯穿于第 3 章所述的评估流程。

ISCM 项目评估并不是为了验证组织及其业务/任务流程和系统对于 SP800-137 所提出的各种 ISCM 概念的实现情况，而是为了确定这些概念以及 FISMA 和 OMB 对联邦组织提出的 ISCM 要求是否可充分判断 ISCM 项目的稳健性[7]（Robustness）。应注意的是，各组织或评估人员根据本指南制定 ISCM 项目评估方案时，可能会根据自己对重要性的认知而制定出不同的评估标准。

2.1 ISCM 管理

ISCM 首先是整个组织的责任，然后是系统级责任【SP800-37】，还包括任务/业务流程。组织范围内的持续监控工作的第一步是组织领导制定全面的组织级 ISCM 战略，该战略不仅要为风险管理部门（RE（f））决策提供直接支持，还要包括与组织各风险管理级别相关的统一管理指标[8]。仅当 ISCM 战略在组织层面上制定实施，并与 RE（f）建立内在联系时，才能保证 ISCM 项目具有合理的广度和深度，为组织各层级明确划分职责。组织级战略由系统级 ISCM 战略和任务/业务流程 ISCM 战略（可选）提供支持。

CM 包括执行持续监控功能的所有人员、策略、流程、技术和标准，它是一个赋能过程，在组织面临网络安全威胁和风险时为组织提供支持，维持正常运营。

合理的 ISCM 项目会规定组织各层级的活动，保证 ISCM 功能在全组织范围内实施。要有效支持整体 ISCM 工作，须统一开发、部署和维护 ISCM 活动，这些活动要能反应整个组织的 ISCM 战略目标和风险管理战略。

以下各节介绍了重要的 ISCM 概念，说明了 ISCM 项目评估与各个概念的相关性。有关制定和实施 ISCM 的更多信息，参见 SP800-137。

2.1.1 ISCM 背景

ISCM 目标包括检测组织的运营、系统环境中的异常与变化、洞悉资产情况、发现漏洞和威胁、了解安全控制的有效性以及安全态势。要实现 ISCM 目标，要在 ISCM 架构中部署工具和技术，结合使用手动和自动方法，按照合理频率提供满足具体需要、详略得当的信息。ISCM 项目的关键成果是收集、集成、分析和呈现整

---

[7] 用于 ISCM 项目时，“稳健性”是指 ISCM 能力足够准确、完整、及时和可靠，能够向组织决策者提供安全状况信息，使其能够做出基于风险的决策。

[8] [SP800-39] 定义了组织风险管理级别：组织级（级别 1）、任务/业务流程级（级别 2）和系统级（级别 3）。

个组织的所有系统及其运行环境的安全相关信息，促进基于风险的决策[9]。

有效的 ISCM 项目会区分组织级 ISCM 战略中的手动和自动监控过程，将这些过程和输出进行关联，最终呈现态势感知结果。使用手动过程前要进行验证，保证过程可复用，实施结果一致。

自动化过程（包括使用自动化支持工具）可以使持续监控更为统一，效率更高，结果更准确，成本效益更高。

有效的 ISCM 项目可推动系统持续授权和再授权决策【SP800-37】，如 2.1.7 节所述。在持续监控期间收集的安全相关信息可用于更新各适用系统的授权包和支持工件。更新后工件作为证据，可证明基线控制措施按照最初计划为系统提供了持续保护。

2.1.2 ISCM 流程各阶段

NIST SP 800-137 将 ISCM 流程分为六个阶段，如图 1 所示。具体信息见如下段落。有一点要注意，对于覆盖全组织的信息安全持续监控工作或流程，第一步都是开发全面的 ISCM 战略，涵盖技术、流程、程序、运行环境和人力等各方面因素。

图 1：ISCM 流程

ISCM 分为六个阶段，在本文中称为“流程阶段”，具体如下：

- **定义 ISCM 战略（定义）** – 根据风险承受能力，定义全组织和系统级 ISCM 战略，保持对资产、漏洞、最新威胁信息和任务/业务影响的清晰认识。根据全组织 ISCM 战略，为组织内部的各个系统定义系统级 ISCM 战略。任务/业务流程领域若需定义 ISCM 战略，也须与组织级战略一致，用于支持任务/业务流程领域的系统。
- **建立 ISCM 项目（立项）** – 建立 ISCM 项目，确定指标、状态监控频率、控制评估频率和 ISCM 技术架构。
- **实施 ISCM 项目（实施）** – 实施 ISCM 项目，收集指标、评估和报告所需

[9] 对于联邦机构来说，利用覆盖整个联邦政府的统一 ISCM 方法，OMB 和 DHS 才能从整体上评估联邦政府的安全态势。这一道理同样适用于非联邦组织。

的安全相关信息。尽可能采用自动化方法收集、分析及上报数据。

- **分析 ISCM 数据并出具报告（分析/报告）** – 分析收集的数据，报告监控中发现的问题，确定合理的响应措施。有时可能需要收集额外的信息，以澄清或补充现有的监控数据。
- **响应 ISCM 中发现的问题（响应）** – 通过技术、管理和运营风险缓解活动响应所发现的问题，或接受、转移/分享或避免/拒绝风险。
- **回顾、更新 ISCM 项目和战略（回顾/更新）** – 回顾、更新监控项目，调整相应级别的 ISCM 战略，完善测量能力，提高资产可见性和对漏洞的感知能力，进而基于数据来管控组织的信息基础设施安全，提高组织的恢复能力

ISCM 的“定义”阶段定义了组织级、系统级和任务/业务流程级（可选）ISCM 战略。RMF 在针对 1 级和 2 级的“准备”阶段阐述了组织级和任务/业务流程级（可选）ISCM 战略，在针对 3 级“选择”阶段阐述了系统级 ISCM 战略（见 SP800-37）[10]。

2.1.3 组织的风险管理级别

ISCM 适用于 SP800-39 中定义的所有三个组织风险管理级别[11]：

- **1 级（组织级）：** 管理整个组织的风险，将风险背景信息和风险决策传达给 2、3 级风险管理者。
- **2 级（任务/业务流程级）：** 基于从 1 级风险管理获取的风险背景信息、风险决策和风险活动，从任务/业务流程角度管理风险。
- **3 级（系统级）：** 是组织内部面向系统的风险管理级别。这一级侧重于系统活动，以 1、2 级风险管理中所输出的风险背景、决策和活动为指导。

在 3 级风险管理过程中获取的安全相关信息和采取的相应措施传达至 1 级和 2 级，用于组织级和任务/业务流程级风险决策。ISCM 项目评估验证了不同级别之间的信息流。

2.1.4 NIST 风险管理框架与 ISCM

根据 SP800-37 定义，RMF 是一个结构化的有序过程，它将信息安全和风险管理活动融入到组织和系统的系统开发生命周期中。ISCM 项目的实施依赖于 RMF 中实施的工件和过程，同时也为 RMF 各阶段提供输入，促进对风险的了解和管理。评估方法和评估要素要虑及所有可能出现的重叠和/或关系。

RMF 的“监控”阶段涉及持续监控，这是风险管理流程的关键环节。ISCM 的实施可以满足组织持续监控的要求，这一过程中产生的输出可用于识别、应对风险。另外，组织也应该监控其整体安全架构以及相应的安全计划，确保即使发生了变化，整个组织的业务仍处于可接受的风险水平之内。及时、相关、准确的安全相关信息

---

[10] “级别”一词取自 NIST [SP800-39]。
1 级按照组织的战略目标以及联邦法律、指令、政策、法规、标准和任务/业务功能所规定的要求建立、实施治理结构，从*组织的*角度管理风险。本文档中，1 级风险管理由负责整个组织总体风险战略、政策和程序的人员实施。
2 级设计、开发和实施任务/业务流程，用以支持 1 级定义的任务/业务功能，从*任务/业务流程*的角度管理风险。本文档中，2 级风险管理由负责子组织任务/业务流程 ISCM 战略、政策和程序的人员实施，该子组织与具体的任务/业务流程而非整个组织相关。
3 级风险管理活动反映组织的风险管理战略，与支持组织任务/业务功能的单个系统的成本、计划和性能要求有关的任何风险都纳入该级管理。在本文档中，3 级风险管理责任归属于为具体系统实施 ISCM 的人员。

[11] NIST SP 800-37（修订版 2）将“*层级*”（Tier）更名为“*级别*”（Level）。在即将更新的 NIST SP 800-39 中，“*层级*”也会更新为“*级别*”。

至关重要，在资源缺乏时尤其如此，组织必须重点关注此类信息。

就 3 级而言，RMF 的“监控”阶段与 ISCM 活动高度一致。对所实施安全控制措施的评估方法相同，不管评估仅是为了支持系统授权（RMF 的“授权”阶段），还是为了支持更广泛、更全面的持续监控工作。系统级主管和员工进行持续评估，监控并分析结果。组织级、任务/业务流程级和系统级的风险管理都要用到该信息。

尽管频率要求不尽相同，无论哪个级别，只要获取到最新的安全相关信息，就能应用于受影响流程。在 ISCM 项目范围内执行的 RMF 监控活动为系统风险判断提供持续支持，是持续授权（OA）的基础。若 ISCM 项目足以支持对整个（或部分）组织的风险进行判断，则能够支持整个（或部分）组织的 OA。ISCM 项目评估可验证相关 ISCM 结果（有时包括相关指标）是否提供给 OA 流程用以就系统授权做出决策。OA 相关信息见 2.1.7 节。

2.1.5 治理与 ISCM

ISCM 治理是整个组织治理的一部分，通过确立权限、职责、责任以及治理流程和程序，推动 ISCM 治理流程的落实、实施和持续改进，进而监控组织安全。治理—包括 ISCM 治理—在整个组织的各风险管理级别建立了责任线。

ISCM 治理是一种用于管理风险的概念性组织和规划结构。它与一个或多个高管或员工相关，如 RE（f）等受问责制约束的高级官员（如负责风险管理的高级问责官员、高级机构信息安全官（SAISO）、负责隐私的高级机构领导、首席信息官（CIO）等）。信息安全治理结构中涉及 ISCM 的部分与其他治理结构一致，以确保与组织内的现有管理实践相兼容，提高总体效率。

ISCM 项目评估可确认 ISCM 治理政策和流程是否到位并实施。在 1 级风险管理中，评估可确认高管是否认识到管理信息安全风险的重要性并建立了与 ISCM 相关的治理结构用以管理此类风险。组织级 ISCM 战略涵盖 ISCM 治理结构。

如果组织的治理结构分散（例如，由于任务/业务需求或运营环境分散），任务/业务流程领域（2 级）在与组织级 ISCM 战略保持一致的同时，可以完整或部分地制定本领域的 ISCM 政策和流程，特别是当它们与风险管理和信息安全决策相关时。对于分散式治理模型，组织各级别共享 ISCM 信息很重要，因为这些信息与风险管理决策相关。

2.1.6 ISCM 指标

ISCM 确定的指标可揭示组织的整体安全态势和各个系统的安全状况，为风险管理流程提供输入。有关 ISCM 指标[12]的更多信息，参见 SP800-137。

ISCM 项目评估涵盖组织定义的指标。ISCM 项目评估会检查 ISCM 项目是否进行了指标的定义、开发、维护并确保指标具有持续性。ISCM 项目评估还会检查组织是否：（i）确定了指标数据的收集频率；（ii）根据 1、2、3 级风险管理获得的数据定义指标；以及（iii）根据需要将指标应用于基于风险的决策。此外，ISCM 项目评估还会检查 ISCM 指标是否已上报给各级指定官员审查。

2.1.7 持续授权

ISCM 可促进 OA，这对组织来说是一大益处。OA 简化了系统授权流程，支持更高的自动化能力，方便相关人员就是否继续系统授权做出近乎实时的决策。根据定义，OA 指根据组织的任务/业务要求和组织的风险承受能力，以商定频率（有成文规定）进行的后续风险判断和风险接受决策。从根本上说，OA 与对安全风险的持续理解和接受有关，并且依赖于稳健的 ISCM 项目。

组织通过 ISCM 功能收集安全相关信息，再基于此信息对系统做出 OA 决策。

[12] 有关指标开发的更多信息，请参阅 SP800-55《信息安全效能评估指南》。

稳健的 ISCM 项目会定义、建立和实施一个连续的过程，通过这个过程，使用手动、自动和程序工具来管控操作授权系统的风险。

ISCM 项目评估会检查是否有 ISCM 信息可用于 OA 决策。ISCM 项目评估具体检查如下各项：

- 是否有组织级 OA 流程。OA 流程关注的是系统如何过渡到 OA 状态以及系统保持 OA 状态所需的条件。
- 所进行的控制措施评估（根据 NIST SP 800-53A）是否足以按既定频率支持 OA。
- ISCM 项目提供的指标是否足够稳定、可靠，可以支撑 OA 决策。
- ISCM 项目是否能够监控系统的安全状况以及这些系统持续运行的环境，监控频率是否合理，足以就是否继续在组织内运行系统做出基于风险的持续决策。
- 是否将 ISCM 结果上报给有关领导进行授权决策。

2.2 ISCM 项目评估的基础

通过 ISCM 项目评估，组织领导能了解组织 ISCM 项目的有效性和完整性。ISCM 项目评估结果应反映组织（整个组织、任务/业务流程或系统）满足评估标准的程度。评估结果能揭示 ISCM 项目的充分性和一致性，还可能包括对 ISCM 项目设计、实施、运营和治理的改进建议。

ISCM 项目评估过程包含信息收集和证据分析。组织可利用所收集的信息和已确认的证据进行如下活动：

- 识别改进组织 ISCM 项目（包括 ISCM 战略）的具体机会；
- 判断组织领导或员工对 ISCM 项目以及该项目在风险管理流程中所处位置的了解程度；
- 判断组织对 ISCM 项目在各级别的适用性以及 ISCM 功能在全组织集成度的了解程度；
- 识别组织安全和风险管理项目的潜在改进机会，包括 ISCM 能力与组织风险管理功能之间的联系；
- 重点考虑与组织 ISCM 项目相关的风险应对决策和相关风险缓解活动；
- 确认组织已解决系统和运行环境中识别出来的安全问题和缺陷；
- 支持监控活动和信息安全态势感知；
- 评估持续授权的准备情况；
- 为未来或计划中 ISCM 项目的设计提供指导或评估现有 ISCM 项目中所做的计划性变更。

ISCM 项目评估以评估要素及其使用为基础，ISCM 项目评估人员基于此对 ISCM 项目做出评判。ISCM 项目评估围绕评估要素，确定 ISCM 能力是否能够满足或在多大程度上满足了 ISCM 要求和目标。

ISCM 项目评估会检查通用控制措施、混合控制措施和特定系统控制措施的控制评估流程，判断组织是否对控制措施进行了评估。本文并未要求在评估 ISCM 项目时评估单个控制措施或检查控制措施的评估结果。必要时，组织可修改 ISCM 项目评估方案、增加评估要素来评估单个控制措施，也可引入控制评估流程。本章其余部分将逐一解释 ISCM 项目评估的各个环节。

2.2.1 ISCM 项目评估标准

ISCM 项目评估方案为评估 ISCM 项目定义了各个方面的评估标准（如安全状况监控政策和程序、通用控制措施评估政策、配置管理程序、安全状况报告）。本文档定义的评估标准以评估要素为核心。ISCM 项目评估要素是对 ISCM 项目各种属性的陈述，由评估人员逐一评审。所有的 ISCM 项目评估要素都基于 2.1.2 节所述的 ISCM 流程阶段。这些 ISCM 项目评估要素及其属性均在一览表中列出。以下是评估要素示例：

- 有基于组织级 ISCM 战略建立的 ISCM 项目。（评估要素 1-002）
- 有组织级安全状况监控政策。（评估要素 1-008）
- 按照规定频率和程序进行安全状况监控。（评估要素 3-007）
- 有组织级政策要求将 ISCM 结果输入到风险评估流程。（评估要素 1-011）
- 按照程序，对 ISCM 项目发现的风险进行响应措施确定和优先级设置。（评估要素 3-023）
- 有 ISCM 指标及相应评审程序。（评估要素 2-024）
- 回顾 ISCM 战略，确定如何提高已知和新型威胁响应能力。（评估要素 6-005）

若 ISCM 相关陈述的来源跨越多个 ISCM 阶段，则要分成多个评估要素，每个（唯一）要素对应一个流程阶段。评估要素也会从其他 ISCM 功能和原则中提取，如开发人员、操作人员、评估人员根据经验和联邦指导所建议的功能和原则。

本文档提供的一览表列举了 ISCM 项目的各评估要素，是综合 ISCM 项目评估所需的最小要素集合。然而，评估可能受到 ISCM 流程阶段数量或风险管理水平的限制。有些 ISCM 流程阶段会跳过，评估要素集中会剔除相应评估要素，然后再提交给评估人员。

要素的选择取决于评估范围（见 2.3.2 节），评估范围受 2.1.2 节中定义的风险管理级别或 ISCM 流程阶段的限制。例如，评估范围受限情况下，按如下原则选取评估要素：

- 对于 1 级风险管理，仅选择适用于 1 级的要素。注意：适用于 1、2 级的要素和适用于 1、2、3 级的要素都在这个集合中。
- 对于“定义”和“立项”阶段，从一览表或组织定义的评估要素集中仅选择适用于 ISCM 流程阶段 1 和 2 的要素。注意：每个要素只适用于一个流程阶段，多个阶段连续进行，无论何种情况，“定义”阶段均不可省略。

有些评估要素会评估 RMF 过程所输出信息（如当前风险水平、风险承受水平、威胁和漏洞信息）的使用，因而在一定程度上超出了 ISCM 项目的范围；有些要素则评估 ISCM 项目是否能够输出安全相关信息（如安全状况报告、安全指标），为组织实施 RMF 提供参考；还有些评估要素可能与 SP800-53 中某些控制措施重叠，但 ISCM 项目评估并不考虑或评估个别控制措施的有效性。

组织或评估人员可以基于本文档提供的评估要素和评估程序，制定自己的评估方案，输出评估 ISCM 项目所需的证据，判断评估标准所规定的 ISCM 要求是否已实现。

评估要素也可以视为对当前所开发 ISCM 项目的要求。组织可根据这些要素，设计 ISCM 项目所需的功能、政策和程序。评估要素还可用于评估 ISCM 规划或设计，如 ISCM 技术架构、操作步骤和 ISCM 战略。

2.2.2 ISCM 项目评估要素来源

- ISCM 项目评估要素的来源包括：
- 2014 年《联邦信息安全现代化法案》（FISMA）【FISMA2014】；
- 行政指令，包括白宫计划和行政命令；
- 涉及 ISCM 要求的 OMB 备忘录【OMB M-11-33】；
- OMB 通知 A-130（2016）【OMB A-130】；
- NIST 风险管理指南和 ISCM 指南【SP800-37】【SP800-39】【SP800-137】；
- 从 ISCM、安全工程、网络安全、系统工程和信息技术等集体从业经历所获取的专业经验。

各种来源均完整收录在附录 C 中，并在一览表的“源”属性列中列出。注意：在对 ISCM 项目评估时，一个评估要素可能有多个来源。

ISCM 项目评估要素一览表【一览表】包含 128 个评估要素，每一要素条目均包含评估程序等属性。共有 89（70%）个评估要素源自 SP800-137，39 个（30%）源自其他文件。

2.2.3 ISCM 项目评估要素属性

每一 ISCM 项目评估要素均有多个属性，方便评估 ISCM 项目的实施情况。在 ISCM 项目评估要素一览表中，这些属性按列展示，具体如下：

- ISCM 项目评估要素 ID
- ISCM 项目评估要素描述
- 风险管理级别
- 来源
- ISCM 项目评估程序
- 备注 – 为 ISCM 项目评估程序属性提供的补充信息
- 级别说明
- 父要素 – 前一阶段的 ISCM 项目评估要素
- 链标签
- 链分类

各 ISCM 项目评估要素都在“备注”属性栏提供了补充指导信息，用以对评估要素进行判断，对含糊的评估要素描述、潜在评估对象、特定对象的关注点进行澄清，提供补充信息的来源。“备注”属性及其相关说明，见 3.3 节。

2.2.4 ISCM 项目评估要素一览表

ISCM 项目评估要素一览表是一个信息库，提供了 ISCM 项目评估所定义的所有评估要素。一览表中，每个评估要素占用一行，其属性按列展示。

2.2.5 ISCM 项目评估要素追溯关系（链）

可将 ISCM 项目评估要素串成链，这样，基于 ISCM 项目的特定方面（如安全状况监控或 ISCM 指标），可方便地从一个要素追溯到与“父要素”属性相关的一个或多个其他要素。评估要素串联在一起，构成“链”，提供追溯关系。这种关系链可显示跨越两个或多个 ISCM 流程阶段的要素的上下级关系。

评估人员针对各风险管理级别检视或调查评估对象时，会发现通过追溯链来追踪评估要素的路径很方便。例如，针对某一评估要素链的工件或面谈问题只关注某一特定领域（如 ISCM 战略），有助于评估人员做出更有效的判断。

图 2 显示了四个类似评估要素的追溯链，这些要素都来自“定义”阶段（要素 1-032）。各要素左上角的字符串是该要素的唯一标识（第一个数字字符表示 ISCM 流程阶段）。

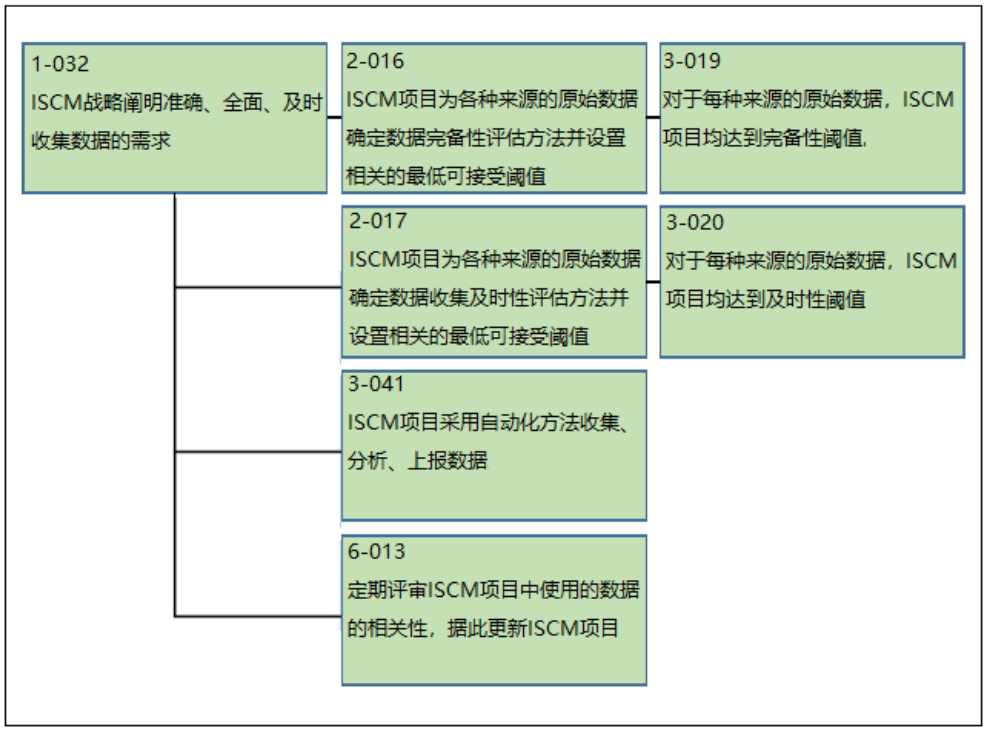

图 2：追溯链示例

在图 2 中的追溯链示例中，第一条链由评估要素 1-032、2-016 和 3-019 组成，涉及 ISCM 相关数据的完备性。第二条链由评估要素 1-032、2-017 和 3-020 组成，涉及 ISCM 相关数据的及时性。第三条链由 1-032 和 3-041 组成，涉及数据的自动化处理。第四条链由 1-032 和 6-013 组成，涉及使用这些数据回顾、更新 ISCM 项目。

在第一条链中（即 1-032、2-016 和 3-019），第一个区块与第二个相连，第二个又与第三个相连。评估人员可根据各评估要素的描述和具体情况，要求提供能反映数据完备性的工件。然后，基于这些工件对这三个评估要素做出判断。第二条链中，子链（2-017 和 3-020）的父区块（1-032）与第一条链相同，但这些区块评估的是数据收集的及时性。评估人员可要求提供能反映数据收集及时性的工件。与第一条链一样，工件随后可用于对链中的三个评估要素做出判断。第三条链的情况类似。评估人员可要求演示自动化功能或提供有关自动化的文档工件。对于第四条链，评估人员可要求组织提供工件，说明如何使用数据来评估 ISCM 项目。

追溯链图表包含在[一览表]中。这些图表反映了 ISCM 的各个方面，如 ISCM 战略管理、指标、控制评估严格性等。按不同方面或领域（即追溯链）对要素进行评估时输出的信息会很有用，尤其是就某一方面（如 ISCM 相关指标）进行评分或者是需要识别该方面不足时更是如此。

2.2.6 ISCM 项目评估特点

ISCM 项目评估涵盖 ISCM 项目的各个方面，以 SP800-137 中的原则为基础。ISCM 项目评估有如下特点：

- 一次只针对一个 ISCM 流程阶段；
- 每一评估要素仅适用于一个 ISCM 流程阶段；
- 使用现成的安全相关信息（如组织级或系统级 ISCM 战略文件中的信息）；
- 不评估控制措施的有效性，因为这超出了 ISCM 项目评估的范围[13]；
- 验证 ISCM 项目是否能够将自动和手动方法结合使用；
- 将每一评估要素追溯至权威来源或 ISCM 专业经验；
- 评估人员或组织可根据需要添加评估程序，修改评估标准（即“评估要素描述”属性），或添加、排除、修改评估要素的属性字段，如 3.5 节所述；
- 适用于任何组织，无论规模多大，结构有多复杂；
- 与技术、实现和独特的组织或项目要求保持分离和独立；
- 输出结果，提出可行建议；
- 从战略和项目角度进行评估，而不是纠结于 ISCM 期间发现的具体的、战术性的问题；
- 足够清晰，指导性够强，保证评估方案可复用（也就是说，其他评估团队进行后续评估也会产出相同结果）。

2.2.7 基于评估标准评估 ISCM 项目

ISCM 项目评估方案包含一个框架，用于评估人员对评估要素做出判断。本节概述了判断的类型和方式。

对于 ISCM 项目的某一方面（如 ISCM 战略或 ISCM 输出/报告），根据相关评估要素（见 2.2.5 节有关追溯链的描述）进行评估。对于每个评估要素，评估人员选取预定义的判断值，做出判断。判断值示例见下文。

对于 ISCM 项目评估范围内的评估要素集，所有要素都要进行判断。有关 ISCM 项目的评估范围，见 2.3.2 节。

- **判断值**

判断值并不是固定的，取决于组织的需要和评估人员能够实现的评估粒度级别。虽然本指南中未规定评估的具体判断值，但根据 NIST 指南，判断值集默认包含两个值，即“满足”或“未满足”，相当于“对/错”[14]。

对于默认判断值集，评估过程中的每一判断语句（见 3.3 节）产生一个判断值：“满足”或“未满足”。评估中提供注释或说明，对“未满足”判断进行解释（即评估要素的哪些部分导致无法给出“满足”判断）。例如，注释中可说明哪些 ISCM 方面仅局部完成，方便组织了解已完成的内容和缺失的内容。注意：配套文档【一览表】是基于默认的二元判断集编制的。

组织也可以采用更精细的方法来处理调查结果，在评估中引入“部分满足”类。对于二元判断，注释可以更精细，对“未满足”判断给出更细致的原因（见 3.3.2 节）。注释可对不产生直接判断的条件或情况进行探讨。注释可由工具辅助完成，也可以

---

13 控制有效性评估，见 SP800-53A。

14 “满足”和“未满足”判断值集与 SP800-53A 中阐述的评估结果一致。

在评估期间手动记录。

更细粒度的判断值示例如下：

- 基本/完全如此
- 有时候是
- 既不对也不错
- 基本相反
- 完全相反

该例中，所有的判断都可以注释，即使是“基本/完全如此”，因为这表示该要素基本上反映了现实情况，但又不完全是。对于二元值集或更细粒度的判断值集，组织可以通过注释说明原因：（i）指出不足之处；（ii）指出达到“完全满足”所需采取的进一步措施；（iii）帮助确定潜在响应措施的优先级。评估结果报告中应基于注释内容提供建议。

- **做出判断**

3.3 节解释了评估要素并阐述了如何做出判断。ISCM 项目评估要素包含评估要素描述（即评估标准）和一组属性，其中两个属性是“评估程序”和指导判断的“备注”信息。“评估程序”属性由一个或多个从“评估要素描述”中提取的评估目标和可能的评估方法和对象组成。“备注”属性提供了与评估要素相关的补充信息，还可能为评估人员可能需要考虑的特殊情况或依赖关系提供其他详细信息（见 3.3 节）。

获得证据[15]或与潜在利益相关者进行面谈后，评估人员会判断 ISCM 项目是否满足特定评估要素的要求。评估人员从为评估要素定义的判断值中选取一个值作为判断。二元判断集表示评估是否满足，而多元、细粒度的值集表示评估要素的满足程度（如“有时候是”、“基本相反”等）。

图 3 显示了使用可用信息对评估要素进行判断的过程。

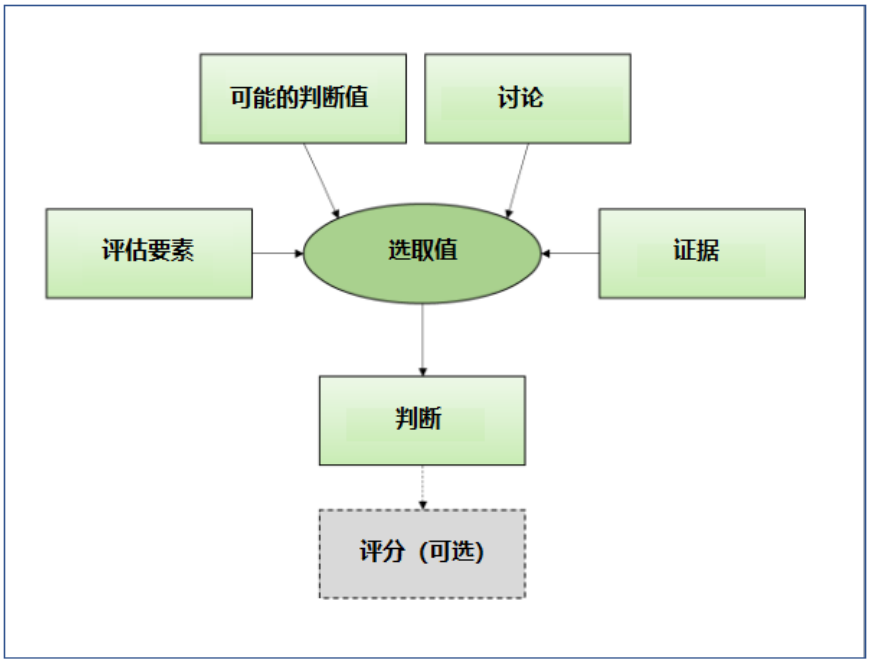

图 3：判断过程

[15] [一览表] 中例举了与评估要素相关的证据，作为与“检查可能的评估方法”相关的潜在评估对象。

- **“不适用”判断**

本文档中未对 ISCM 项目评估定义“不适用”（N/A）判断。要确保所有评估要素尽可能适用于整个组织，这意味着，即使 ISCM 项目未实现 ISCM 项目的某些评估功能或方面（例如，评估中有评估要素评估外部服务，但组织没有使用外部服务提供商），也没有将 N/A 作为判断值。

由于所有评估要素都要关注，而不是为某次评估定制，因此 ISCM 项目评估要考虑如下因素：

- 每个评估要素都要进行判断。
- 如果评估要素的某方面，例如使用外部服务提供商，不适用于组织，则组织级 ISCM 战略要明确说明该方面不适用于该组织。
- 无论组织对该方面作何决策，在 ISCM 项目评估的整个过程都要考虑并评估该方面情况。
- 若组织决定不实施 ISCM 某一特定方面，则意味着不存在相反证据，评估人员将对此进行验证。

若 ISCM 项目评估要素不适用于组织或系统,则应提前在相应战略中予以说明，之后，所有与此相关的要素均判断为“满足”。若战略中没有提及此事，则所有相关要素均判断为“未满足”。

2.2.8 在特定风险管理级别评估 ISCM 项目

根据组织的规模和复杂性，可以从多方面（如多个任务/业务流程和/或系统）收集 ISCM 项目评估信息，对其进行分析和汇总，最后形成单一组织风险管理级别的单个判断。多个评估人员可以就组织的某一部分（如单个任务/业务流程、单个系统）输出多个评估结果。

对于同一风险管理级别的多个 ISCM 项目评估（由多个评估人员进行），组织或评估人员决定如何将同一评估要素的多个判断进行合并。例如，如果评估人员分别接触各任务/业务流程，则可能会对同一评估要素做出多次判断。分布式自评也是如此（见 2.3.1 节）。一个风险管理级别的评估结果可能存在显著差异。对于某一组织风险管理级别，可用如下方法将判断进行合并：

- 最坏情况：采用最坏情况的判断（下限）作为最终结果。
- 少数服从多数：将多数人的判断作为最终结果。如果两种判断势均力敌，则依据预定义规则来确定最终结果（例如，平局时采用最坏情况判断）。
- 评估人员确定：评估人员考虑所有因素，根据经验做出判断。

各评估要素按上述原则在对应风险管理级别分别进行判断。

2.2.9 跨风险管理级别评估 ISCM 项目

SP800-137 介绍了三个风险管理级别如何就 ISCM 的各个方面协同工作。根据组织的结构以及组织级和系统级 ISCM 战略的实现方式，这些概念会适用于一个或两个级别（通常是相邻级别）或所有三个级别。因此，每个评估要素都会在一个或多个级别上进行评估。例如，一个要素可能只在级别 1 进行评估，而另一个要素则可能在级别 1 和级别 2 都要进行评估。对于每个要素，不管涉及几个级别，都要将多个评估结果进行合并，最终形成唯一的判断结果。

当两个或三个级别的判断需要进行合并以得到最终结果时，需要有方法、规则或算法来保证这种操作有统一的标准可循。本文档并未提供合并判断的方法，各组织可根据需要建立自己的合并机制。

每个相关级别都要进行一次或多次评估。如 2.2.8 节所述，在每个级别将结果合并为单一判断。然后，根据组织定义的规则，将各级别的结果进行调整，形成唯一判断。例如，要合并各级别评估结果，可基于后文三个表格中的其中一个决策矩阵采用如下规则：

规则 1：如果评估要素只适用于单个级别，则该级别的判断作为该要素的最终判断。

- 规则 2：如果评估要素适用于两个级别，则使用表 1、表 2 或表 3 中的决策矩阵。
- 规则 3：如果评估要素适用于所有三个级别，则：

  a. 对 2 级和 3 级应用规则 2；然后

  b. 对级别 1 应用规则 2 和规则 3a 的应用结果。

请注意，不一定非要将决策矩阵与上述规则一起使用。有时，可以使用简单的规则来代替，例如，当合并两个判断值时，选择最坏情况的值作为结果判断（或采用少数服从多数[16]等判断方法）。

评估时可使用上述规则 2 或 3 对两个级别进行合并判断，表 1 便是这样一种决策矩阵示例。该例中，使用最坏情况法将具有不同值的两个级别结合起来，得出的结果是四分之三的判断均为“未满足”。

表 1：合并两个级别的判断（无倾向）[17]

低级别	高级别	组合判断（无倾向）
满足	满足	**满足**
满足	未满足	**未满足**
未满足	满足	**未满足**
未满足	未满足	**未满足**

表 2 提供了涉及两个级别的另一种决策矩阵，该矩阵倾向于高级别，能大概反映组织的业务情况。该例中，规则 2 和规则 3 没有变化；但是，不管应用哪种规则，结果都与表 1 矩阵不同。

表 2：合并两个级别的判断（倾向于高级别）

低级别	高级别
满足	满足
满足	未满足
未满足	满足
未满足	未满足

表 3 提供了涉及两个级别的第三种决策矩阵，该矩阵倾向于低级别，更接近组织的实际情况。该例中，规则 2 和规则 3 没有变化；但是，不管应用哪种规则，结果都与表 1 和表 2 矩阵不同。

[16] 基于单一或两个级别的评估判断。

[17] 矩阵中的“高”和“低”指[SP800-39]中所描述的风险管理层级中的位置，最高级别为 1 级，最低级别为 3 级。

表 3：合并两个级别的判断（倾向于低级别）

低级别	高级别	组合判断（倾向于低级别）
满足	满足	**满足**
满足	未满足	**满足**
未满足	满足	**未满足**
未满足	未满足	**未满足**

2.2.10 评分

评估分数表示 ISCM 能力对目标的满足程度，反映组织的风险情况。基于评估要素做出判断后进行评分，用数值描述判断，最后得出评估结果。为每个判断值分配分数，再基于各评估要素分值计算组织的最终分数。换言之，评估得分是所有要素判断得分的总和。

基于该分数，组织领导可就 ISCM 项目做出明智决策，确定如何优化组织资源配置，以便改进项目，降低风险。评分操作非必选项，可与 2.2.7 节中讨论的二元和多级判断类型结合使用。可将全组织的 ISCM 项目评估分数汇总，计算出整个组织的最终分数。

使用默认的二元判断值，为每个评估要素分配一个分值，如表 4 所示。

表 4：默认判断值评分示例

分数	判断
1	满足
0	未满足

根据需要，可以将各评估要素得分乘以一个权重因子（为数值形式）。这种操作后，评分会更高。根据特定要素对组织的重要性，可以为不同的评估要素分配不同的权重。也就是说，组织可制定一个权重分配方案，为不同的优先级分配不同的权重因子。2.2.11 节介绍了可能影响评估要素重要性的各种因素。

与任何类型的数字评分一样，结果可以用百分比表示，方法是将分数除以可能的最佳分数。

2.2.11 重要性[18]

评估要素分为关键要素和非关键要素，对评分方式有不同的影响。符合以下条件的 ISCM 项目评估要素为关键要素：

- ISCM 项目围绕，比如，以下问题：
  a. 国家网络安全问题（例如保护高价值资产[HVA]信息和系统）；
  b. 国家、组织或特定部门的严重、普遍的安全问题，如内部威胁；
  c. 国家网络安全计划（例如持续授权过渡计划、总统网络安全计划等）；
  d. 影响组织业务流程/任务的私有问题。
- ISCM 项目的某一部分为项目的其余部分提供了基础，因而对这部分评估要素的评估具有重要意义，例如，ISCM 战略、政策和程序对评估 ISCM 能

[18] 请注意，[一览表]中提供了重要性，方便用户与[NISTIR8212]对齐。组织可根据组织风险评审重要性并修改值（是或否）。

力的实现和/或运营就很重要。

- ISCM 项目是其他重要商业需求或国家网络安全项目或计划（如 RMF 或网络安全框架[CSF]【CSF 1.1】）的一部分。
- ISCM 项目覆盖各种网络安全功能或责任（例如通用控制）。

在评估过程中，关键评估要素的提法可能会根据国家网络安全优先事项、目标和问题的变化而变化。此外，考虑到各组织的风险承受能力不同，关键评估要素可能因组织而异。

2.2.12 评价结果报告

如果进行评分，ISCM 项目评估结果中包括被评估的整个或局部组织的总分，该总分基于各评估要素评分结果计算得出。报告可以按整个组织、组织各部分、风险管理级别、特定评估要素属性（如评估要素的来源）、各个方面或类别（例如战略、指标、治理、调查结果的重要性）、各评估要素得分或其他组织认可的方式对数据进行分类总结。

评估结果包括根据收集和分析的数据提出的建议。有些建议是评估工具基于判断结果自动生成的，有些建议则是由评估人员通过人工决策提出的。组织或第三方评估人员可基于对评估要素的判断，确定是否给出自己的建议。

根据预期用途，评估结果可以多种方式呈现在评估报告中，例如雷达图、图表和表格。

结果还可以与评分相结合，从多个不同角度展示评估结果。指标形式的结果可上报给不同的组织领导（如 CIO、SAISO、RE（F）、AO 等），以便领导基于风险做出决策。

2.3 ISCM 项目评估实施

ISCM 项目评估的首要目标是为组织提供 ISCM 项目改进建议，从而管理和降低组织所面临的风险。ISCM 项目评估过程有多种描述方法，包括评估类型和评估人员类型、评估深度和持续时间以及预期评估结果。

2.3.1 ISCM 项目评估类型

ISCM 项目评估有两种方式：第三方评估和自评。

第三方评估：第三方评估由独立于被评估组织的第三方评估人员进行，分为以下两种情况：

- 外部人员–评估人员来自独立的外部组织[19]。
- 内部人员–评估人员属于组织，但就评估任务而言，独立于被评估组织实体。

第三方评估通常要组织多次访谈，按以下方式进行：讨论参与者的回答，得出并记录达成一致的结果，例如由评估人员将结果输入工具或结果库。

自评：自评由被评估组织或子组织的内部人员进行，包括分布式评估和引导式评估。自评要求对目标形成客观看法，这样才能在 ISCM 项目开发早期揭示整个或局部组织的 ISCM 能力的不足之处。

自评可分布式进行，方法如下：

- 多名参与者在一名内部员工的领导下同时评估各要素；

[19] 评估人员的独立性是保持评估过程公平公正、确定评估结果可信度以及确保组织领导基于客观信息以做出基于风险的明智决策的一个重要因素。评估人员的独立性级别由组织根据法律、行政命令、指令、法规、政策、标准或指南确定。

- 参与者将一组评估人员的判断直接输入到工具或库中（不一定同时），然后无需讨论就可以手动或通过工具（或半自动程序）计算最终结果。

引导式评估中，一名具有专业领域知识的员工或团队引导小组讨论，然后达成一致并记录下来（例如，将回答输入工具或结果库）。

2.3.2 ISCM 项目评估的范围和持续时间

就流程阶段而言，ISCM 项目评估的范围很灵活。评估可以在任何阶段或逻辑停止点停止，可以评估局部组织而不是整个组织。ISCM 项目评估在评估范围方面具有以下特征：

- ISCM“定义”阶段不能省略，以确保 ISCM 的基础得到评估。
- ISCM 项目评估逐步进行，可在任一阶段后随时停止。例如，评估可以：
  a. 终止于“定义”阶段（重点评估 ISCM 项目战略）；
  b. 终止于“立项”阶段（重点评估 ISCM 项目设计）；
  c. 终止于“实施”阶段（重点评估 ISCM 项目实施）；
  d. 跳过“回顾/更新”阶段（过程改进阶段，在较成熟的 ISCM 项目中进行）；或
  e. 包含所有阶段（完整 ISCM 项目评估）。

ISCM 项目评估具有足够的灵活性，允许在特定的时间点暂时中止评估。暂停评估有多种益处，例如，对 ISCM 项目进行改进后再继续。如果需要，评估人员可帮助组织处理发现的任何问题。

2.3.3 ISCM 项目评估的期望结果

进行 ISCM 项目评估的目的是改善组织的安全态势，降低风险。为此，ISCM 项目评估要输出具有可操作性的建议，从各方面改进 ISCM 项目，包括设计、实施、运营和治理等。ISCM 项目评估的主要输出是调查结果报告，该报告要提交给组织，包括以下内容（如适用）：

- 介绍信息和背景材料（例如评估过程概述）；
- 详细的记分卡（若使用评分）和/或概述组织 ISCM 项目有效性的其他形式的内容；
- 根据评估标准认定的实施效果良好的特定 ISCM 领域；
- 可以改进的特定 ISCM 领域；
- 改进 ISCM 的具体建议以及根据这些建议改进 ISCM 记分卡的具体方法。

此外，被评估组织的员工可单独出具一份评估情况报告提交给评估机构，以便改进 ISCM 项目评估过程。

3. 评估流程

本章介绍了评估的组成部分和 ISCM 项目的总体评估流程。ISCM 项目评估流程明确了组织如何进行 ISCM 能力评估，包括：（i）组织和评估机构为准备 ISCM 项目评估而开展的活动，（ii）ISCM 项目评估计划的制定，（iii）ISCM 项目评估的实施和评估结果的分析和报告，以及（iv）评估后报告分析和后续活动。

3.1 ISCM 项目评估流程概述

成功的 ISCM 项目评估需要考虑组织 ISCM 能力有关各方的需求，包括系统负责人、授权人、首席信息官、首席信息安全官、隐私事务高级机构官员/首席隐私官，首席执行官/机构负责人、安全和隐私工作人员、监察长或其他审计机构、RE（f）和负责风险管理的高级官员。建立评估前、评估中和评估后期望至关重要，可确保获得可接受的结果，即输出必要的信息，便于组织领导判断 ISCM 项目是否足以满足组织的需求，进而影响授权决策，决定是上线新系统还是继续使用当前系统（持续授权）。整个过程如图 7 所示，详细信息见下文。

虽然评估依赖于评估人员手动进行，但会将自动化 ISCM 过程的输入作为证据，进行判断。例如，ISCM 输出的报告可以通过组织仪表盘或安全信息和事件管理（SIEM）组件提供给评估人员；然后评估人员基于该报告对一个或多个特定评估要素做出判断。接下来，评估人员或工具（若有）收集和汇总来自各级别的评估参与者的判断结果，生成针对整个组织的判断，构成最终评估结果的基础。

依据本指南制定的 ISCM 项目评估方法评估的是 ISCM 项目本身，而不是 ISCM 项目的运营结果。ISCM 项目评估的目标不是：（i）重新测试安全控制的有效性或操作程序，（ii）评估 ISCM 实施情况，或（iii）验证 ISCM 项目的特定输出。ISCM 项目评估通常不审查单个控制措施评估的结果，而是检查被评估组织的各部分是否按照 ISCM 战略以组织确定的频率进行控制评估。

理想情况下，ISCM 项目评估流程应可以复用，以确保结果的一致性。通过使用本指南 3.3 节中描述的 ISCM 项目评估要素，可确保评估流程的复用性，为评估人员提供关于潜在评估对象、检查点、单独评估要素的评估目标以及目标面谈人员角色等方面的指导。此外，各 ISCM 评估要素的“备注”属性就如何对评估要素进行判断提供了指导，有的还提供了有效判断值，供评估人员选择。

3.5 节阐述了组织或评估人员如何调整本章提出的方法，根据自己的实际需求进行评估。

> ISCM 项目评估直接评估组织内定义和实施的 ISCM 项目，而不是评估实现 ISCM 能力的单个具体组件，如单个通用控制措施、混合控制措施和特定系统控制措施。ISCM 项目评估验证评估要素某一方面是否到位，例如，验证是否按照指定频率针对特定行动执行了特定程序。ISCM 项目评估不会评估 ISCM 能力的单个自动化功能、手动功能或运营功能。

3.1.1 ISCM 项目评估计划

ISCM 项目评估计划为 ISCM 项目评估的实施提供指导。ISCM 项目评估计划包含 ISCM 项目评估过程计划阶段所作的决策（如 3.2 节所述），方法如下：

- 对于第三方评估，评估团队制定 ISCM 项目评估计划，并提交给组织进行审批。最终版本将在启动会议上交给评估参与者。
- 对于自评，ISCM 项目评估计划由关键评估人员和组织管理层内部制定。ISCM 项目评估计划由组织领导批准，并将根据 ISCM 项目评估结果采取行动。最终版本将在启动会议上交给评估参与者。

ISCM 项目评估计划包括但不限于以下内容：

- 评估类型
- 评估范围
- 人员配置来源
- 评估人员角色及职责
- 时间表与期限
- 关键里程碑
- 按顺序进行和同时进行的活动
- 针对特定组织风险管理级别的评估人员合并判断方法
- 针对多个组织风险管理级别的评估人员合并判断方法
- 后勤信息
- 评估调整决策和实施
- 报告类型（草稿和终稿）

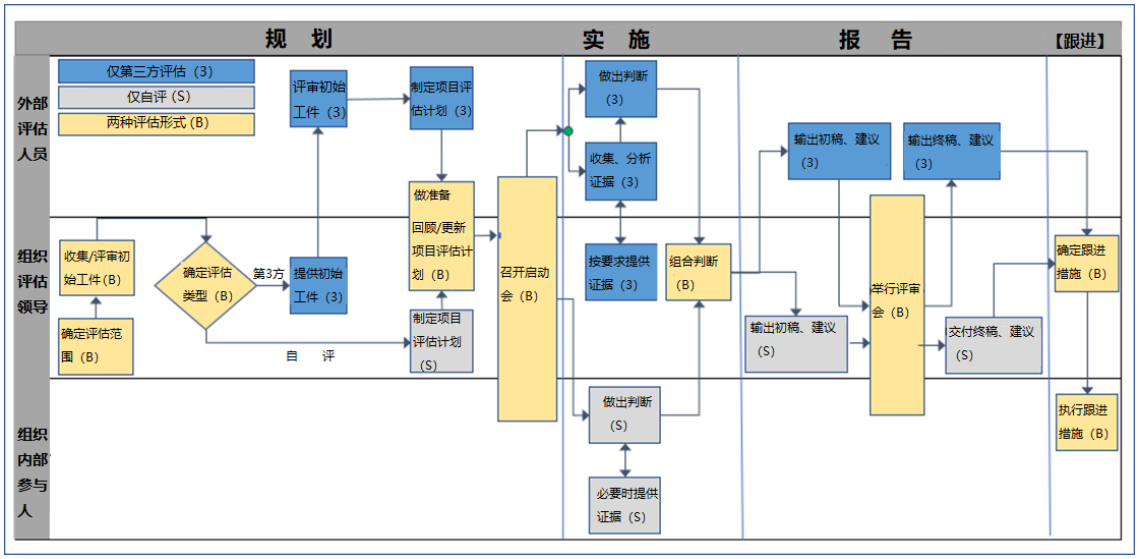

图 4：ISCM 项目评估流程

3.2 ISCM 项目评估流程阶段

ISCM 项目评估由一系列的活动组成，是一种基于现有评估方法的逻辑性、系统性方法。ISCM 项目评估流程有三个阶段：

- ISCM 项目评估规划（规划阶段）
- 进行 ISCM 项目评估（实施阶段）
- 报告 ISCM 项目评估结果（报告阶段）

每次 ISCM 项目评估行动都要根据组织的需要和适用评估要素进行定制。ISCM 项目评估可分为自评和第三方评估，如 2.3.1 节所述。图 4 说明了 ISCM 项目评估三大阶段中的具体活动。

3.2.1 规划阶段

ISCM 项目评估的规划阶段明确了评估过程，并将项目评估的实施进行了固化，如图 5 所示。

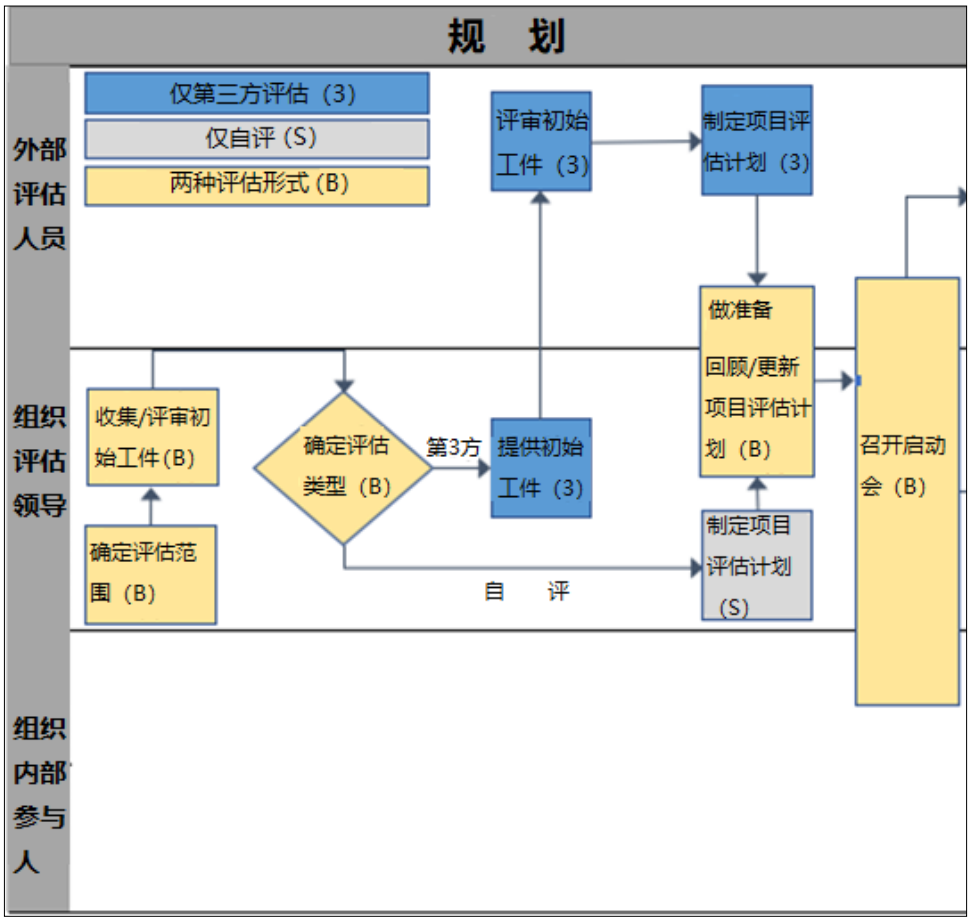

图 5：ISCM 项目评估流程（规划阶段）

规划活动针对一系列重要问题，涉及 ISCM 项目评估的实施方式（自评或第三方评估）、成本、计划表、人员配备和后勤保障。规划假设各评估要素适用于一个或多个组织级别。参与者仅在一个适用级别对一个要素做出一个判断，且这种判断与他/她在其他适用级别所做的判断无关。

要实现全面的 ISCM 项目评估，评估负责人确保 ISCM 的所有领域都由知情员工进行评价，具体如下：

- 进行第三方 ISCM 项目评估的团队成员或了解 ISCM 项目评估范围内的所有能力，或接触过 ISCM 项目评估各领域，具有实操经验。此外，评估人员还需要具有必要的相关技能和经验，确保能够提供准确、一致的判断和实用的改进建议。
- 进行自评的个人对本 ISCM 领域非常了解。

在详细规划之前，需要评审初始的基础工件（例如，组织级 ISCM 战略和组织结构图）。然后，根据初始工件集的相关信息，更新 ISCM 项目评估计划，调整以下内容：

- 组织的行动力
- 被评审的评估对象以及参与人员
- 完成 ISCM 项目评估的期限
- 组织有效管理评估所需的关键里程碑决策点
- 连续活动和并行活动

组织要执行以下关键规划活动：

- 获得组织批准，为 ISCM 项目评估设立一名执行发起人；

- 确定评估的目标、严格性和范围；
- 确保组织领导了解要评估的任务/业务流程，任务/业务流程已拉通，方便评估人员获取评估相关要素所需的信息；
- 上报组织的重要领导，说明即将进行 ISCM 项目评估，分配必要的资源进行评估；

安排启动会；

- 确保 ISCM 相关工件已到位，可供评估人员使用（例如，成文政策和操作程序、计划、规范、设计、记录、ISCM 报告、系统文档、信息交换协议、以往评估结果、法律要求等）；
- 对于自评，确定并从组织中选择具有相关知识的评估人员/团队，同时考虑评估人员的独立性问题。

确定评估范围时，组织可能认为局部评估（如 2.3.2 节所述）较为合适，也就是说，计划会限制待评估组织的流程阶段数量，指定哪些部分将接受评估。该形式被组织批准后，相关工件将提供给评估团队，方便他们在启动会之前检查详细的背景信息，进而缩短评估时间。

评估团队需做如下准备工作：

- 与组织的相关管理人员会面，就 ISCM 项目评估的目标、严格性和范围进行沟通，达成一致；
- 在组织内指定执行 ISCM 项目评估所需的联系人；
- 全面了解组织的运作，包括组织结构、任务、职能、业务流程和员工角色；
- 确定 ISCM 项目评估的重点领域（如问题领域、高优先级/可见性计划）；
- 全面了解任务/业务流程内的系统对评估过程的支持性；
- 了解每个系统的结构（待评估的系统架构）；
- 对于第三方评估，选择有能力的评估人员/评估团队，如果评估人员属于组织（即内部第三方评估），则要考虑独立性问题。

组织和评估领导人共同开展以下活动：

- 规划筹备组织领导和评估人员之间的启动会议；
- 在组织和评估人员之间建立沟通桥梁，尽量减少对 ISCM 实施的模糊认识或误解以及 ISCM 项目评估期间发现的任何不足/缺陷；
- 制定完成评估和定期检查的时间表，监测和管理进度。

启动会议的目的是确认行动决策，回答问题，解决后勤问题以及任何其他问题。与会者包括以下组织人员：组织高级领导（CIO、SAISO/CISO、RE[F]）、任务/业务负责人、系统负责人、系统安全主管、被选中参与或支持 ISCM 项目评估的其他人员，以及行政支持人员，包括后勤和组织联系人。评审机构领导和高级评审人员也会参加启动会议。

3.2.2 实施阶段

ISCM 项目评估按 ISCM 项目评估计划进行，该计划或会在启动会议期间进行修改。要成功进行 ISCM 项目评估，至关重要的是获取欲评审 ISCM 项目和评估范围内系统相关的工件且能够联系上相关组织人员。图 6 说明了 ISCM 项目评估过程的实施阶段。

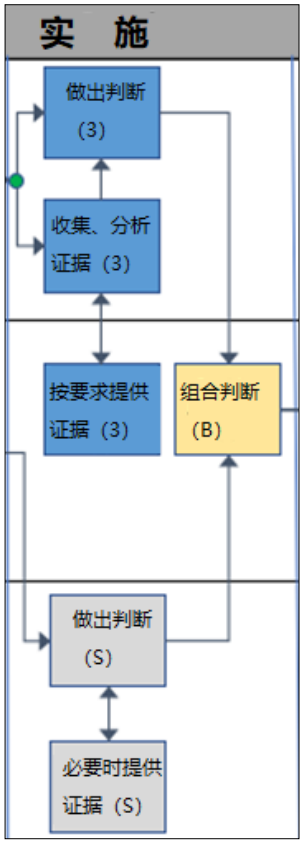

图 6：ISCM 项目评估流程（实施阶段）

实施阶段的目标是了解组织的 ISCM 项目在下列各方面发挥的作用：

- 规划、制定组织级 ISCM 战略以及建立 ISCM 项目；
- 规划、实施可选任务/业务流程 ISCM 战略；
- 为被评估的各任务/业务流程内的所有系统规划、实施系统级 ISCM 战略；
- 实现、运行和维持 ISCM 能力；
- 分析 ISCM 结果，确定组织安全态势；
- 响应 ISCM 结果，降低组织风险；
- 向各级组织通报 ISCM 结果；
- 以组织规定的频率检测所实施控制措施的差距和不足，判断控制措施是否足够有效、可以达到预期目的；
- 回顾、更新和改进 ISCM 项目。

可使用基本的电子表格、PPT 和 Word 文档记录、保存评估要素和评估原始数据并提交评估人员和组织领导。有些商业工具基于特定的评估标准，面向系统和组织项目评估，可用于评估；但是，本文档不为任何商业信息技术产品、应用程序或系统背书。

组织可部署工具进行评估，并以本文中的评估要素作为评估工具以及评估工具需求库的基础[20]。可以开发评估工具来支持判断决策，包括协作方法、Delphi 模型、评估人员投票和调查知情人员。

[20] 例如 ISCMAx 工具，见 NISTIR8212。

- **证据收集**

ISCM 项目评估信息是从组织人员和 ISCM 输出（报告）中获取的，而不是与 ISCM 能力直接交互。根据组织结构、角色和评估范围，对组织各级人员进行访谈，以获取相关信息并对评估要素做出判断。

在收集 ISCM 安全相关信息以了解控制有效性时，自动化是主要方法，但有些控制是手动监控的。所以，ISCM 项目评估还可以从手动收集的数据中获取 ISCM 结果。ISCM 项目评估可获得的证据包括但不限于：

- 文件：
  a. 组织级 ISCM 战略
  b. 组织级 ISCM 政策（可能单独成文，也可能包含在 ISCM 战略中）
  c. 任务/业务流程 ISCM 战略（可选）
  d. 系统级 ISCM 战略
  e. ISCM 实施操作过程
  f. 系统安全计划
- ISCM 通过如下方式输出的安全相关信息：
  a. 仪表板或其他动态监控系统和组件（如 SIEMs）生成的报告
  b. 手动生成的报告
  c. 为各级别领导编写的报告，包括 CIO、CISO、RE（f）员工、AO、任务/业务区域管理人员、通用控制提供商、系统负责人和 ISSO
- 与下列各类人士访谈获得的信息：
  a. 组织领导
  b. 系统负责人和系统安全主管
  c. 系统管理员
  d. 风险管理人
  e. 授权人

如果适用的话，当前 ISCM 项目评估可使用之前的 ISCM 项目评估结果（如监察长报告、审计、漏洞扫描、物理安全检查、先前的安全或隐私评估、开发测试和评估以及厂商缺陷补救活动）。

- **证据分析**

信息收集后由评估人员手动分析，并将结果输入到当前库或评估工具中，用以创建图表。通过信息分析，可以判断 ISCM 项目对各相关评估要素的满足程度。

在各组织级别进行判断，以确定 ISCM 项目对该级别特定评估要素是否充分满足。若参与评估的多个人员或小组在同一级别做出不同判断，则评估人员会将这些判断进行汇总，形成唯一判断，如 2.2.8 节和 2.2.9 节所述。例如，评估人员可以对系统级判断进行汇总，形成唯一判断，涵盖对所有被评估系统就特定评估要素做出的所有判断。

在 ISCM 项目评估工作中，评估人员会审查工件，与员工面谈，分析收集到的信息。每天结束时，可与相关组织联系人进行简短讨论，以澄清和确认所发现的问题，进一步提出问题，并确认第二天的活动。

系统级 ISCM 项目评估可以由系统开发人员、系统集成商、安全控制评估员、

系统审计员、系统负责人、组织的安全人员以及 AO 和 AO 人员实施或支持。ISCM 项目评估人员将所有被审查系统的可用信息汇集在一起。如有必要，评估人员可通过修改评估要素的评估程序和方法来增强系统级评估，收集 ISCM 项目相关系统的额外或特殊信息

任务/业务流程 ISCM 项目评估可由任务/业务负责人、通用控制供应商、安全控制评估员和 CISO 员工安全专家实施或支持。组织级 ISCM 项目评估可由组织的 CIO、SAISO/CISO 和 RE（f）员工实施或支持。

在各组织级别对某评估要素做出唯一判断后，根据需要对这些判断进行合并，形成最终判断。当对所有要素都做出唯一判断后，实施阶段结束。

3.2.3 报告阶段

报告阶段（图 7）是评估人员参与的最后一个阶段。ISCM 项目评估的报告阶段定义了 ISCM 项目评估的输出成果。

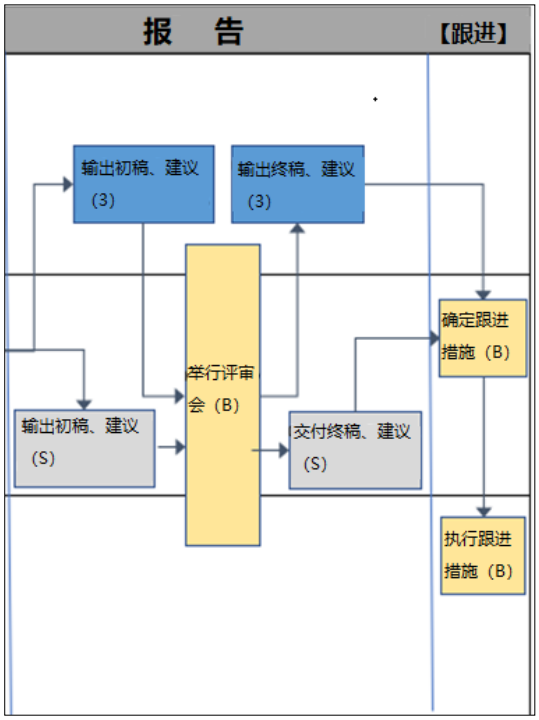

图 7：ISCM 项目评估流程（报告阶段）

在评估的报告阶段，评估人员起草评估报告初稿。ISCM 项目评估结论由评估人员根据分析信息手动得出。评估人员根据 ISCM 项目评估的结论，提出 ISCM 项目的改进建议，这些建议可在非“满足”（或“正确”）项的评估判断注释中提供。评估过程输出定性结果和建议，帮助组织集中精力改进 ISCM 项目。组织会收到一份报告初稿，内容包括调查结果和提供的建议。报告初稿由组织领导（包括执行发起人）审查，以修订错误并澄清误解或含糊之处。根据组织的反馈，评估人员更新报告，形成终稿。ISCM 项目评估报告见 2.2.12 节。

- **评估后响应（跟进）**

组织负责对 ISCM 项目评估结果进行响应。组织需要分析 ISCM 项目评估报告终稿中的调查结果，确定合理响应措施，根据组织的风险承受能力确定响应行动的优先级，并指定角色负责执行响应行动，明确完成时间。计划好的响应行动可以记录在系统、任务/业务流程或组织级行动计划和里程碑中，或以组织要求的格式记录。根据调查结果和组织对调查结果的响应，相应更新 ISCM 项目相关文件（如 ISCM 战略、政策等）。组织还可以重新评估相关 ISCM 项目评估要素，验证已完成的响应行动。

3.3 ISCM 项目评估要素

ISCM 项目评估要素定义了适用于所评估 ISCM 项目各个方面的评估标准。为了确定是否“满足”ISCM 项目评估要素，评估人员需要使用相关评估程序来获取和审查证据。同一组织级别的所有评估要素适用同样的评估程序。

针对特定评估任务添加或修改 ISCM 项目评估要素时，评估程序信息也要相应增加或修改，同时，其他属性（如“备注”）信息也需要添加或修改。关于如何定制 ISCM 项目评估过程以及评估要素，见 3.5 节。

ISCM 项目评估要素能够促进 ISCM 项目评估过程的可重复性，并提供了必要的灵活性，以便根据范围、组织结构、政策和程序、操作考虑、系统和网络架构以及风险承受能力定制评估方案。

3.3.1 评估要素信息字段

评估要素的信息字段，包括评估要素的上下文信息或属性[21]，定义如下：

- **ID**：唯一标识评估要素并代表 ISCM 阶段序号（见 2.1.2 节）的有序字符串。
- **评估要素描述**：为评估 ISCM 项目某一方面而定义的评估标准。评估要素描述是评估人员用来确定目标是否达成目标或目标达成程度的说明。
- **级别**：SP800-39 中定义的适用组织风险管理级别。将 ISCM 评估要素应用于组织风险管理级别的更多信息，见 2.1.3 节。
- **来源**：ISCM 项目评估要素所参考的权威出版物或实践。
- **评估程序**：评估程序属性包含多个部分，规定了评估人员需要执行的一系列操作，以便收集证据，确定评估目标是否已实现。每个评估程序包括（i）一个评估目标，（ii）多个可能的评估方法，以及（iii）ISCM 项目评估所针对的对象，具体如下：

  a. 评估目标：评估目标是与评估要素描述相关的判断语句。判断语句（即“确定是否……”）针对的是评估要素描述的内容，用以确定 ISCM 项目的相关内容是否满足该要素来源中规定的基本 ISCM 原则/要求，或对这些原则/要求的满足程度。应用评估程序对 ISCM 项目的某一方面评估后会输出评估结果，表示是否满足了评估要素或对评估要素的满足程度。

  b. 可能的评估方法和对象：评估程序还对建议的评估方法和适用对象提出了规范要求。评估方法定义了评估人员活动的性质和范围。可用于 ISCM 项目评估的可能方法包括：

     ♦ 检视：审查、检查、观察、研究或分析一个或多个评估对象的过程。检视的目的是促进理解，澄清误解，获取证据。

     ♦ 访谈：与个人或小组进行讨论以促进理解、澄清误解或获取证据的过程。

  组织和评估人员协调行动，获取证据，证明组织为保障[22]ISCM 项目有效性所做的努力。在所有三种评估方法中，证据都用于基于判断语句做出具体判断，以确认评估程序的目标。

[21] 一览表中，属性按行显示在各单元格中。

[22] [SP800-53A] 介绍了评估过程中的安全保障。

评估对象是应用评估方法的潜在项目（证据）。评估对象包括规范、机制输出、活动和个人，帮助评估人员判断 ISCM 项目的某个方面是否满足评估要素或对该评估要素的满足程度。规范是文档型构件，包括：

- ISCM 战略
- ISCM 项目政策和程序
- 系统安全计划
- 安全需求
- ISCM 自动化功能规范
- ISCM 技术架构设计

机制输出是系统或操作环境中使用的特定软硬件或固件监控功能或防御措施所生成的报告或通知，例如：

- 安全仪表盘报告
- SIEM 报告
- 网络防火墙报告

活动是人类参与的与系统相关的监控活动，例如：

- 执行手动监控操作
- 评审 ISCM 报告
- 按程序行事
- 做出基于风险的决策

- **备注：**“备注”属性为评估人员提供各方面的补充指导，包括评估要素、特定对象检查点建议、补充信息/参考资料的来源等。“备注”提供的特殊情况或依赖性方面的补充信息可供评估人员参考。
- **级别说明：**将评估要素分配到特定风险管理级别的理由。
- **父要素：**父要素表示与上一流程阶段评估要素的联系，父要素与当前要素评估的是相同的 ISCM 方面或主题。“定义”阶段要素没有父要素。
- **NISTIR 8212（ISCMAx 工具）中的关键要素：**评估要素可分为关键要素和非关键要素，对评分方式有不同的影响。为方便用户使用，本栏与 NISTIR8212 一致。组织可根据组织风险评审重要性并修改值（是或否）。
- **链标签：**ISCM 项目评估要素可以联结在一起，提供可追溯性，对相关要素进行分组，形成一条链（见 2.2.5 节）。每个链标签提供一个简短的描述性名称，代表一组相关的 ISCM 项目评估要素。
- **链分类：**用于对评估要素进行分类的字符串，以便将它们归并到对应链中，按流程阶段在链内进行排序。

组织不需要采用评估程序中包含的所有评估方法和对象；相反，可以灵活选择方法和对象，并确定评估所需的工作量和所需的保障（即哪些评估方法和评估对象对于获得预期结果最有效）。

表 5 显示了评估要素一览表【一览表】中所定义的评估要素及其属性的格式。

表 6 提供了一览表中的一个评估要素示例。

3.3.2 评估要素的使用

用于 ISCM 项目评估的各评估要素【一览表】由评估人员评估（执行）。如前所述，评估要素的主要对象是评估程序。评估目标是对评估要素的再次说明，评估人员须判断 ISCM 项目的某一方面对该要素的满足程度。

评估要素的评估目标中的每个判断语句（如表 6 所示）会产生一个二元判断值（见 2.2.6 节）：满足或未满足。“满足”表示对于在评 ISCM 项目部分，获得的评估信息（即收集的证据）表明该评估要素的评估目标已达成并产生了可接受的结果。对于“未满足”结果，要在注释中提供判断理由（即，评估要素的哪些部分阻止给出“满足”判断）。注释中提供的判断理由有助于组织了解 ISCM 项目中的不足之处，进而对症下药。“未满足”结果也可能表明评估人员无法获得足够信息基于判断语句做出判断。

对于“未满足”的评估结果，组织可以选择定义子类别，表明发现的缺陷或不足的严重性或重要性以及对组织的潜在不利影响。这有助于确定所需风险缓解措施的优先级。无论组织是否定义了子类别，评估结果都要提供缺陷的充分信息，说明下一步需要采取哪些行动以完全满足判断条件。

表 5：评估要素格式

ID	评估要素描述	级别	来源	评估程序	备注	级别说明	父要素	NISTIR 8212/ISCMAx 工具中的关键要素	链标签	链分类
标识符	评估要素描述	适用风险管理级别	评估要素参考的权威来源	评估目标 判断是否达成目标。 可能的评估方法和对象 检视：规范 访谈：人员	澄清或补充信息或提供给评估人员的额外指导	说明评估要素分配给特定风险管理级别的理由	与前一评估流程阶段的联系	是或否	一组相关 ISCM 项目评估要素的描述性名称	对评估要素按分类字符串，用以按流程阶段排序链内要素排序

表 6：评估要素示例

ID	评估要素描述	级别	来源	评估程序	备注	级别说明	父要素	NISTIR 8212/ISCMAx 工具中的关键要素	链标签	链分类
1-002	有基于组织级 ISCM 战略建立的 ISCM 项目。	1 级	NIST SP 800-137	评估目标 确定是否有基于组织级 ISCM 战略的 ISCM 项目。 可能的评估方法和对象 检视：组织级 ISCM 战略、ISCM 政策和程序文件、ISCM 设计文件、ISCM 运营概念（CONOP） 访谈：1 级：SAISO、ISCM 联系人（POC）	ISCM 项目由基于组织级 ISCM 战略的 ISCM 政策和程序组成，包括指导 ISCM 实施的 ISCM 文件（如 ISCM 技术架构和 ISCM CONOP）。	1 级负责定义 ISCM 项目	“定义”阶段没有父要素	否	ISCM 项目管理	03.01-002

下图举例说明如何基于表 6 中的示例要素使用评估要素。

使用示例评估项信息

步骤 1 到步骤 4 解释了如何使用表 6 中的示例评估要素的信息字段来对示例评估要素做出判断。

- 对于 1-002 **评估要素**：

  有基于组织级 ISCM 战略建立的 ISCM 项目。

  按下述方法对对象使用可能的评估方法：

  a. **检视**：组织级 ISCM 战略、ISCM 政策和程序文件、ISCM 设计文件、ISCM CONOP

  b. **访谈**：SAISO、ISCM POC

  获取证据，对下述 ISCM **评估目标**作出判断：

  确定是否有基于组织级 ISCM 战略的 ISCM 项目。

- 根据需要，使用与“定义”**阶段**和检视列表及访谈列表中的级别 1 相关的信息来确定 ISCM **评估目标**是否达成。
- 使用**备注**：“ISCM 项目由基于组织级 ISCM 战略的 ISCM 政策和程序组成，包括指导 ISCM 实施的 ISCM 文件（如 ISCM 技术架构和 ISCM CONOP）”，澄清评估要素的含糊表述或目的。
- 判断评估要素的满足程度（“满足”或“未满足”），将判断结果输入评估工具或结果库。对于“未满足”判断，在注释中给出理由。

图 8：使用示例评估项信息

对于各适用组织级别，一览表中各评估要素的应用方式大同小异。如 2.2.9 节所述，评估要素适用于多个级别时，评估结果（判断）在组织的多个级别进行合并。本文档一览表中提供的评估要素大多不会告知评估人员如何做出实际判断（例如，“满足”或“未满足”），因为满足 ISCM 项目评估要素的标准可能因系统、任务和组织而异。在评估程序中，评估人员先将评估方法应用于建议对象（证据），再根据评估目标进行判断决策。这里所说的“应用评估方法”是指验证评估要素描述中提及的领域或主题（例如战略、政策、程序、后序行动和 ISCM 报告）。以图 8 所示的方式进行 ISCM 项目评估时，对各要素每评估一次，ISCM 项目评估过程就重复一次。【一览表】

3.4 ISCM 项目评估要素的限制

评估【一览表】包含了 ISCM 项目评估要素的最小集合，组织和评估人员可添加评估要素；如果 ISCM 项目评估受到 ISCM 流程阶段数量的限制（见 2.3.2 节），对于特定的 ISCM 项目评估任务，可删除或跳过某些评估要素。关于定制 ISCM 项目评估过程的详细信息，见 3.5 节。

ISCM 项目评估不重复或增加控制评估（按【SP800-53A】规定操作），但会验证控制评估是否根据各评估要素的条件（例如以指定频率）进行。

3.5 定制 ISCM 项目评估流程

定制是评估人员和被评估组织之间为满足组织需求而进行的合作过程。评估流程各阶段（如 3.2 节所述）和评估任务可以定制。通过定制，可将评估任务与组织的特殊情况对齐，例如，ISCM 项目不成熟时，可进行有限（增量）评估。对于针对整个组织的评估项目，定制后，不同的子组织可根据不同的风险环境确定不同的实施程度。评估要素和评估程序有足够的灵活性，可以根据组织的需要进行调整。

根据组织对 ISCM 项目的具体实施情况，可能需要定制 ISCM 项目评估方案。例如，在为联邦机构定制评估方案时，要保证方案有助于确定组织的 ISCM 项目是否符合有关部门对联邦机构的 ISCM 要求。定制 ISCM 项目评估方案时须与评估机构协调，确保 ISCM 项目评估能够按照要求验证 ISCM 的各方面。所有定制决策都要记录在 ISCM 项目评估计划中。

调整 ISCM 项目评估范围。在定制活动开始时，应确定 ISCM 项目的评估范围，例如针对 ISCM 项目的实施要评估哪些系统和系统组件（用户端点、服务器、网络组件等），以提供可信的评估证据。

调整 ISCM 项目评估范围要了解组织的 ISCM 要求和约束，并在必要时修改评估要素。例如，可根据组织结构（子组织的数量和规模等）或 ISCM 成熟度（如任务/业务流程之间的 ISCM 成熟度差异）进行调整。

评估范围由组织领导决定。如 2.3.2 和 3.4 节所述，可从一览表中选取部分评估要素，以缩小范围（例如，进行小范围评估或根据 ISCM 流程阶段的数量进行增量评估时）。评估范围也可限定于特定的风险管理级别（例如，仅 1 级[组织]范围或仅 3 级[系统级]范围）。

修改评估要素。定制评估方案可能会要求对评估要素的字段/属性进行修改。新技术带来新概念时，可对评估要素进行修改以反映这种变化。如 2.2.7 节所述，评估要素集可通过新增或修改要素进行定制。

如果 ISCM 项目评估中用到某个工具，而根据设计用途该工具并不适用于修改后的某些评估要素及其属性，那么对这些评估要素的修改可能会带来问题。

3.6 ISCM 项目评估结论

ISCM 项目评估可为组织提供 ISCM 项目设计、实施、运营和治理等方面的改进建议。评估结束时，评估人员提交报告初稿，与组织领导讨论并解决意见分歧，最后提交报告终稿。有关报告 ISCM 项目评估结果的更多信息，见 2.2.12 节和 3.2.3 节。

ISCM 项目评估过程有时会很紧张和短暂，有时会很轻松。评估结束后，组织人员可能会与评估团队进行会谈。后续合作中也可能会有这种会谈。

评估后行动。ISCM 项目评估可按预定的时间间隔重复进行，例如当组织的 ISCM 项目制定过程中出现某些里程碑时，或当先前评估的响应行动完成、确认行动结束后。随着组织 ISCM 项目的成熟，后续评估的范围可能会扩大。

参考资料

[44 USC 3544] 美国法典第 44 篇第 3544 节，定义。2006 年编辑 https://www.govinfo.gov/app/details/USCODE-2008-title44/USCODE- 2008-title44-chap35-subchapIII-sec3544

[Catalog] 国家标准与技术研究院（2020），ISCM 评估程序一览表. https://csrc.nist.gov/publications/detail/sp/800-137a/final

[CNSSI 4009] 国家安全系统委员会（CNSS）（2015）术语表.（国家安全局，马里兰州米德堡）CNSS 说明（CNSSI）4009. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[CSF 1.1] 国家标准与技术研究院（2018），提升关键基础设施网络安全框架，1.1 版.(国家标准与技术研究院，马里兰州盖瑟斯堡）. https://doi.org/10.6028/NIST.CSWP.04162018

[FISMA2014] 2014 年联邦信息安全现代化法案，公法 113–283，128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283

[ISCMA Reqs] 国土安全部信息安全持续监控评估（ISCMA）要求.

[NISTIR8212] 待定（【即将出版】）信息安全持续监控项目评估方法，（国家标准与技术研究院，马里兰州盖瑟斯堡），NIST 跨部门或内部报告（IR）8212 初稿.出版后可在下述网址查看：https://csrc.nist.gov/publications

[OMB A-130] 行政管理和预算局（2016），将信息作为战略资源进行管理，（白宫，华盛顿特区），OMB 通知 A-130,2016 年 7 月 28 日. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A13 0/a130revised.pdf

[OMB M-11-33] 行政管理和预算局（2011），联邦信息安全现代化法案与机构隐私管理报告说明，（白宫，华盛顿特区），OMB 备忘录 M-04-04,2011 年 9 月 14 日. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2 011/m11-33.pdf

[SP800-37] 联合特遣队（2018），信息系统与组织风险管理框架：安全与隐私系统生命周期方法，（国家标准与技术研究院，马里兰州盖瑟斯堡），NIST 特刊（SP）800-37，修订版 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP800-39] 联合特遣队转型计划（2011），管理信息安全风险：组织、任务、信息系统视角，（国家标准与技术研究院，马里兰州盖瑟斯堡），NIST 特刊（SP）800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP800-53] 联合特遣队转型计划（2013），联邦信息系统与组织的安全和隐私控制，（国家标准与技术研究院，马里兰州盖瑟斯堡），NIST 特别刊物（SP）800-53，修订版 4，包含截至 2015 年 1 月 22 日的更新. https://doi.org/10.6028/NIST.SP.800-53r4

[SP800-53A] 联合特遣队转型计划（2014），联邦信息系统与组织的安全和隐私控制评估：制定有效的评估计划，（国家标准与技术研究院，马里兰州盖瑟斯堡），NIST 特别刊物（SP）800-53A，修订版 4，包含截至 2018 年 12 月 14 日的更新. https://doi.org/10.6028/NIST.SP.800-53Ar4

[SP800-55] Chew E, Swanson M, Stine K, Bartol N, Brown A, Robinson W（2008），信息安全效能评估指南，（国家标准与技术研究院，马里兰州盖瑟斯堡），NIST 特刊（SP）800-55. https://doi.org/10.6028/NIST.SP.800-55r1

[SP800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM（2011），联邦信息系统和组织的信息安全持续监控（ISCM），（国家标准与技术研究院，马里兰州盖瑟斯堡），NIST 特刊（SP）800-137. https://doi.org/10.6028/NIST.SP.800-137

附录 A 缩略词

本文使用的缩略词列举如下：

AO	Authorizing Official	授权人
CISA	Cybersecurity and Infrastructure Security Agency	网络安全与基础设施安全局
CISO	Chief Information Security Officer	首席信息安全官
CIO	Chief Information Officer	首席信息官
CSF	Cybersecurity Framework	网络安全框架
FISMA	Federal Information Security Modernization Act	联邦信息安全现代化法案
ISCM	Information Security Continuous Monitoring	信息安全持续监控
ISSO	Information System Security Officer	信息系统安全主管
NCCoE	National Cybersecurity Center of Excellence	国家网络安全卓越中心
NIST	National Institute of Standards and Technology	国家标准与技术研究院
NISTIR	NIST Interagency or Internal Report	NIST 跨部门或内部报告
RE(f)	Risk Executive (function)	风险主管（职能）
RMF	Risk Management Framework	风险管理框架
OA	Ongoing Authorization	持续授权
OMB	Office of Management and Budget	行政管理和预算办公室
SAISO	Senior Agency Information Security Officer	高级机构信息安全官
SIEM	Security Information and Event Management	安全信息和事件管理
SISO	Senior Information Security Officer	高级信息安全官

附录 B 术语表

方面	与被评估ISCM项目的某一部分相关的评估要素所针对的领域或主题。
评估	根据上下文，分别指： 针对组织、任务/业务流程、一个或多个系统及其环境的已完成或规划好的评估行动；或 用于单次评估的工具、模板或工作表。
评估要素	特定ISCM流程阶段中要评估的特定ISCM概念。
评估要素属性	适用于某一评估要素的信息项，如评估要素来源或评估要素所适用的风险管理级别。
评估要素描述	对于正常实施的ISCM项目的准确陈述，是评估要素的评估标准部分。
评估方法 **【SP800-53A】**	评估人员在评估过程中为获取证据所采取的方法（检视、面谈、测试）。
评估目标 **【SP800-53A】**	判断语句，即对安全控制措施、隐私控制措施或控制加固措施进行评估时期望获得的结果。
评估程序 **【SP800-53A】**	评估目的集合及相关评估方法与评估对象集合。
一览表	所有评估要素的集合。
链	反映ISCM同一方面的两个或多个关联的评估要素。在阶段1“定义”中，每条链都有一个称为“根”的评估要素，它没有前置要素或父要素。
持续监控 **【SP800-37】**	实时了解威胁信息，为组织风险决策提供支持。
分布式自评	最不正式的评估类型；对各要素的判断基于并行工作的小组的评估。
要素	对于正常实施的ISCM项目的某一ISCM概念的准确陈述。
评估标准	用于评估技术和运营实施有效性或适用性特征的标准。评估标准是衡量技术能力、活动、产品或计划一致性、效能和适用性的基准、标准或因素。

外部评估行动	由第三方评估组织主导的正式评估活动。
引导式自评	与内部评估相比，引导式评估不那么正式，由参与者就特定级别的各个要素达成共识后对要素形成判断。
高价值资产	潜在或现有对手特别感兴趣的信息资源、任务/业务流程和/或关键程序。
内部评估行动	组织内部团队主导的正式评估活动，目的是对评估要素做出判断。
信息安全持续监控（ISCM）项目【SP800-137】	为基于组织战略、政策、程序和预定义指标收集信息而建立的项目，项目所利用的部分信息通过实施安全控制措施获得。
信息安全持续监控（ISCM）战略	ISCM项目建立战略。
判断	从预先配置的评估选项中选择一项与特定组织级别上下文中的要素关联。
判断值	可用于判断收集的信息是否满足某一评估要素的预定义值。
父评估要素	前一流程阶段中的评估要素，是当前要素的上层要素。
专业经验	ISCM评估要素的来源，具体指（1）在设计、实施和运营ISCM能力方面有经验的个人（从业者）；和（2）安全工程经验。
流程阶段	NIST SP 800-137中定义的ISCM流程中的6个阶段。
风险主管（职能）【SP800-37】	组织内的个人或团队，其职责是确保：（i）就组织为完成任务、履行业务职能而制定的整体战略目标，从组织高度考虑各信息系统的安全风险以及对这些系统的授权决策；（ii）统一管理整个组织的信息系统风险，管理时考虑到组织的风险承受能力，同时还要考虑影响组织任务/业务成功的其他风险。

风险管理框架（RMF）阶段	NIST SP 800-37中定义的风险管理框架过程中的6个阶段。
风险管理级别	NIST SP 800-39中定义的三个组织级别：1级（组织级）、2级（任务/业务流程级）和3级（系统级）。
风险承受能力【SP800-137】	实体为实现潜在期望结果愿意承受的风险水平。
稳健性【CNSSI 4009】	就ISCM项目而言，“稳健性”是指ISCM能力足够准确、完整、及时和可靠，能够向组织决策者提供安全状况信息，使其能够做出基于风险的决策。 信息保障（IA）实体在各种运行条件下正确、可靠地运行以及发生意外时的故障恢复能力。
安全控制措施【SP800-53】	为信息系统或组织设计的一种防御措施或对策，旨在保护其信息的机密性、完整性和可用性，满足各种安全要求。
高级机构信息安全官（SAISO）【44 USC 3544】	负责依照《联邦信息安全管理法案》（FISMA）履行首席信息官的职责，并作为首席运营官与机构授权人、信息系统负责人和信息系统安全主管之间的主要联系人。注：SAISO也称为高级信息安全官（SISO）或首席信息安全官（CISO）。
高级信息安全官（SISO）	见“高级机构信息安全官（SAISO）”定义。
系统安全主管（SSO）【SP800-37】	由高级机构信息安全官、授权人、管理人员或信息系统负责人指派的个人，负责保证信息系统或程序的运行安全。
定制【基于SP800-53进行了修改】	类似于SP 800-53中描述的定制基线概念，是一种协作过程，通过以下方式对评估要素集进行局部修改：（i）更改评估范围或风险管理级别；（ii）增删评估要素；或（iii）修改评估要素的属性。

附录 C 追溯链

本附录就一览表中的评估要素提供了追溯链（见 2.2.5 节）。图中各要素左上角的字符串表示评估要素的唯一标识。

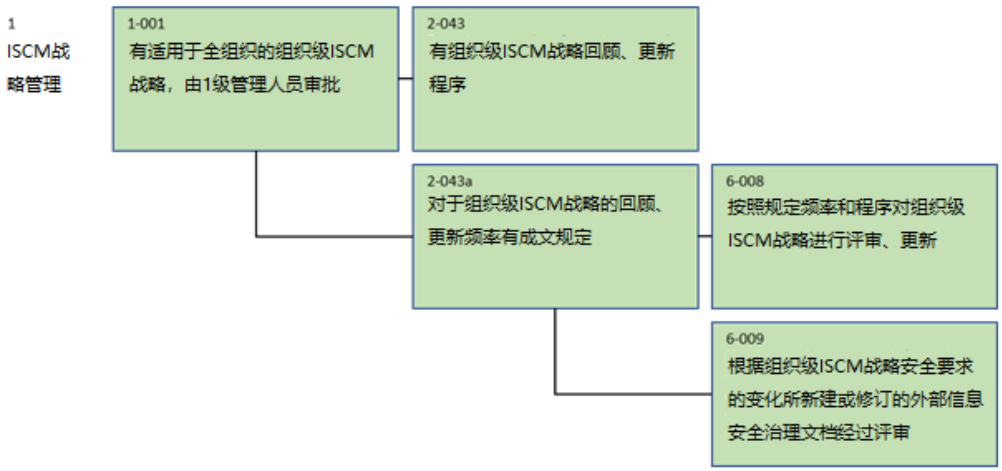

图 9：ISCM 战略管理追溯链

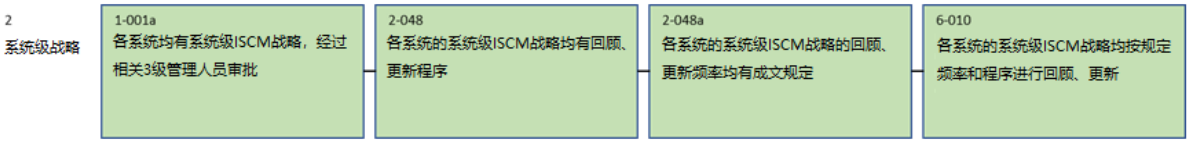

图 10：系统级战略追溯链

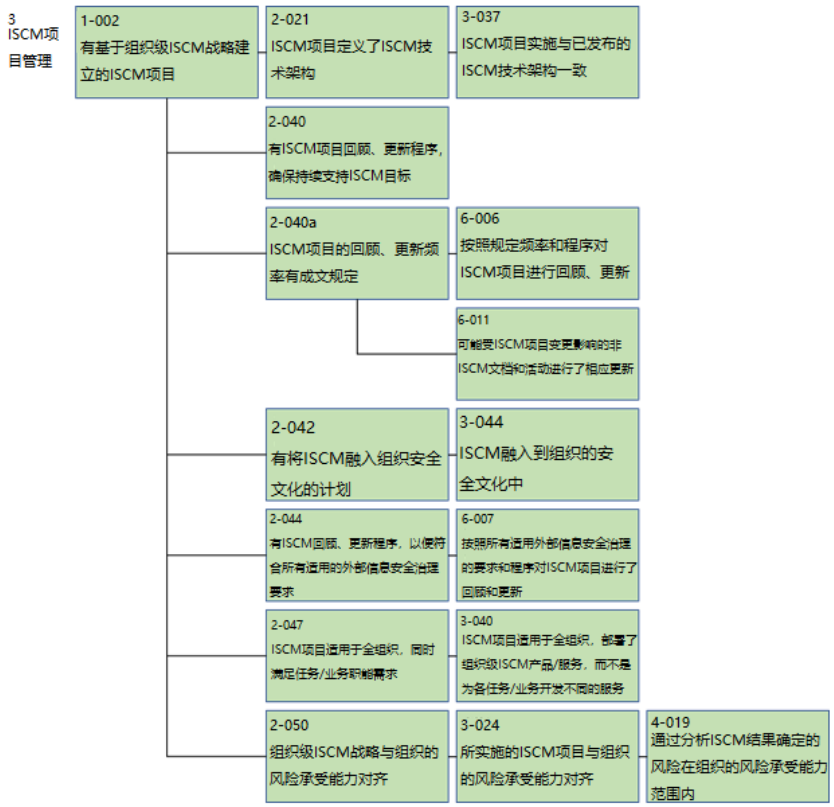

图 11：ISCM 项目管理追溯链

图 12：控制措施评估严格程度追溯链

图 13：安全状况监控追溯链

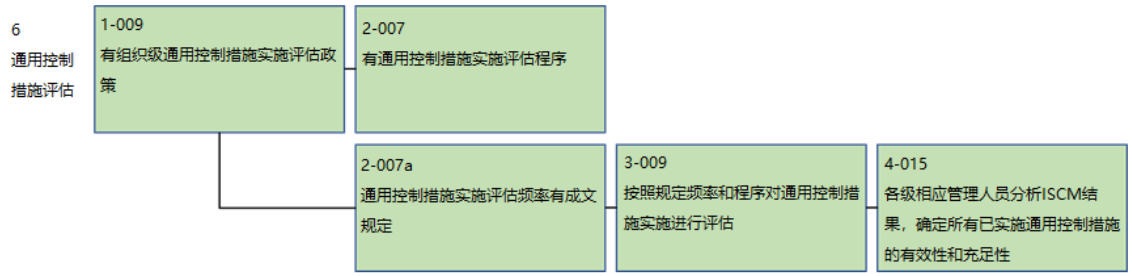

图 14：通用控制措施评估追溯链

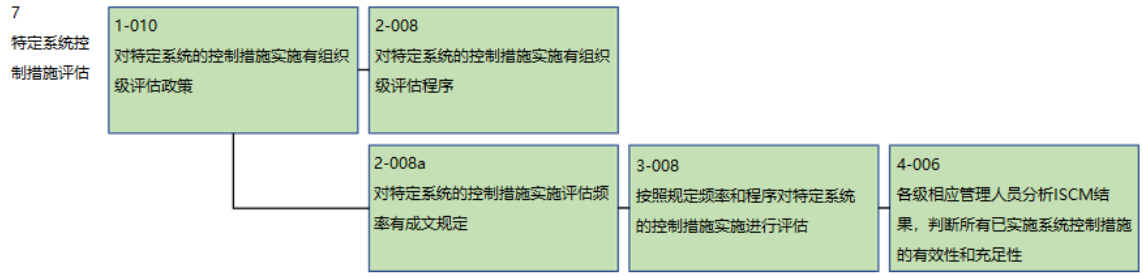

图 15：特定系统控制措施评估追溯链

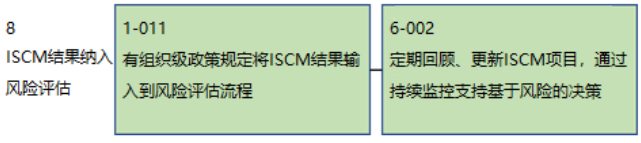

图 16：ISCM 结果纳入风险评估追溯链

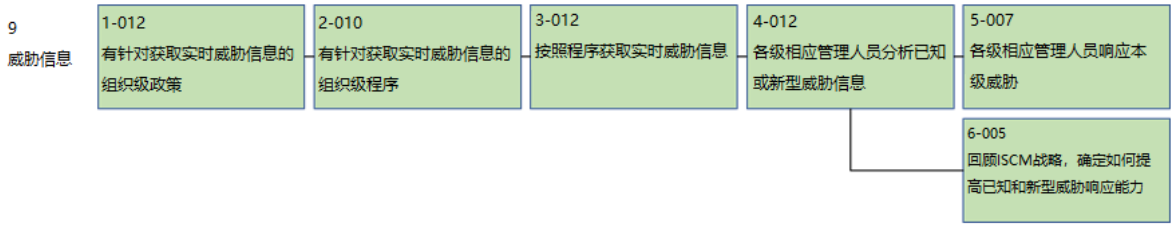

图 17：威胁信息追溯链

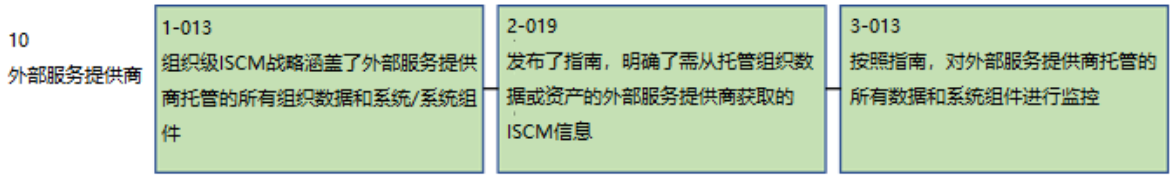

图 18：外部服务提供商追溯链

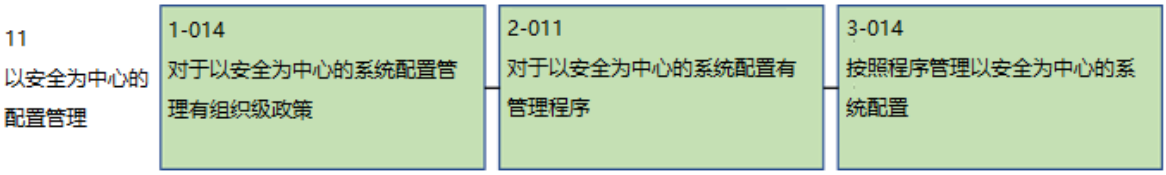

图 19：以安全为中心的配置管理追溯链

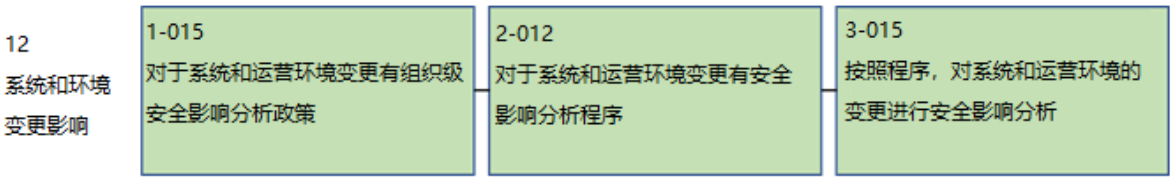

图 20：系统和环境变更影响追溯链

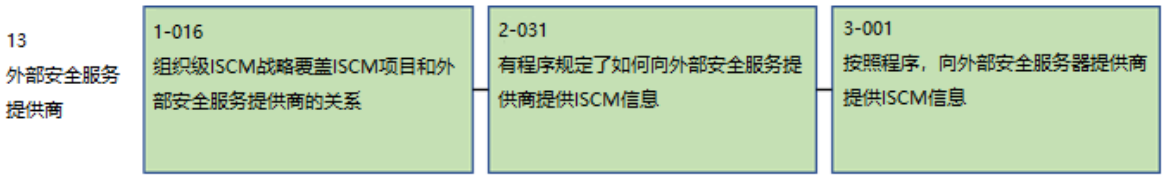

图 21：外部安全服务提供商追溯链

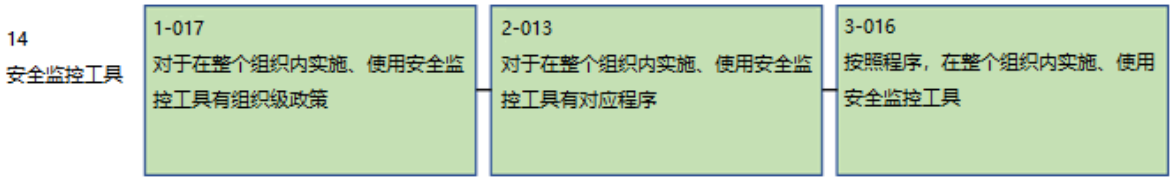

图 22：安全监控工具追溯链

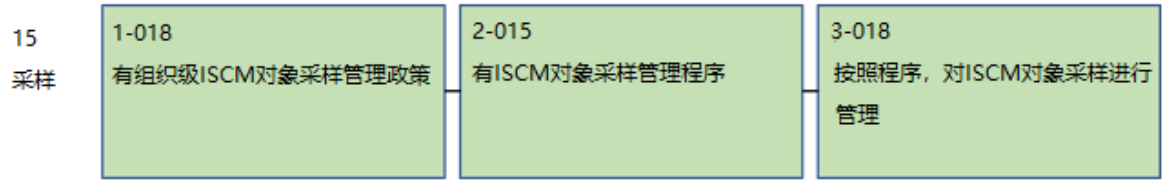

图 23：采样追溯链

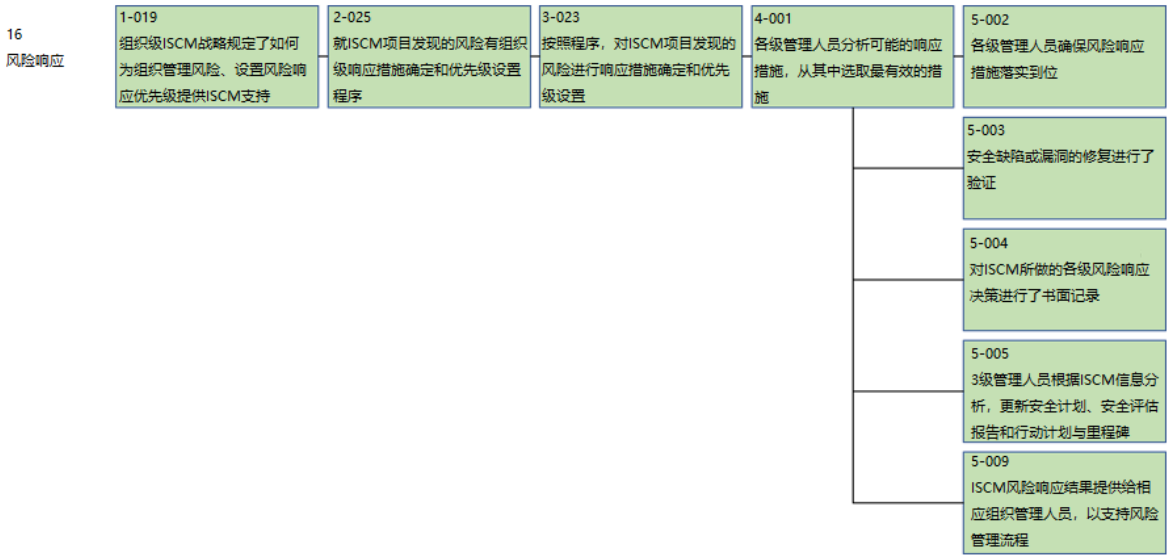

图 24：风险响应追溯链

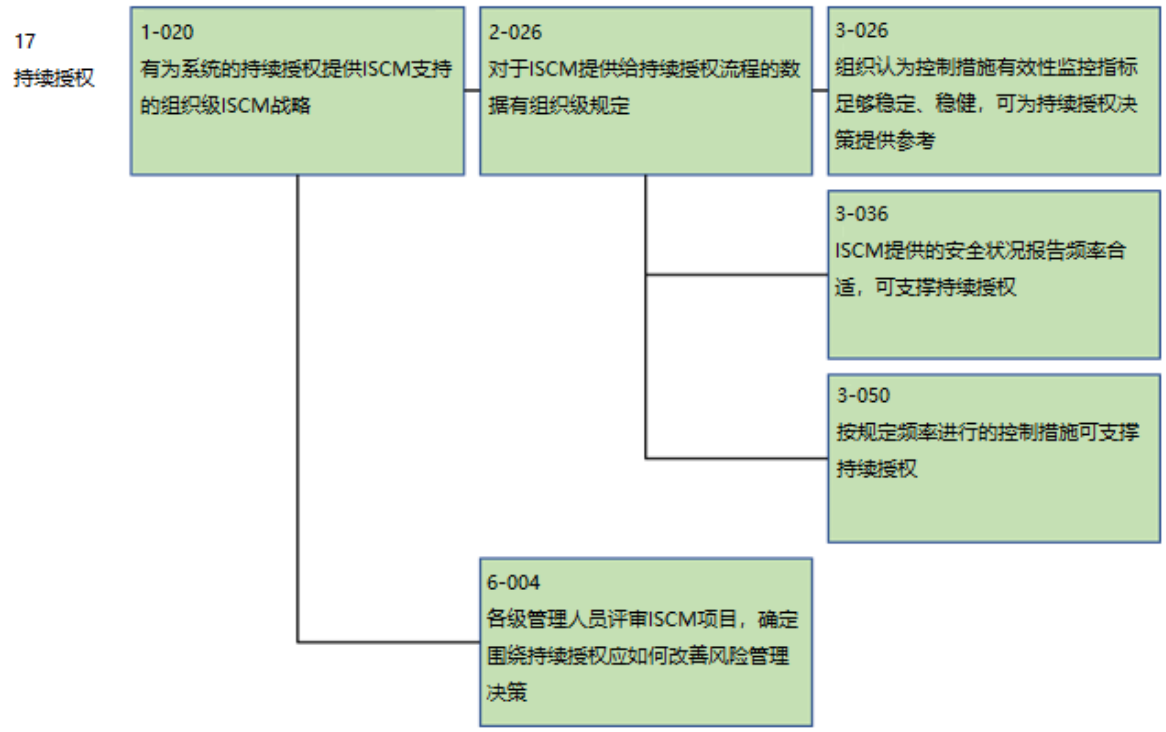

图 25：持续授权追溯链

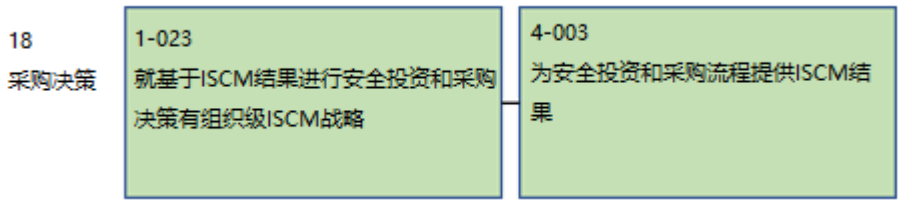

图 26：采购决策追溯链

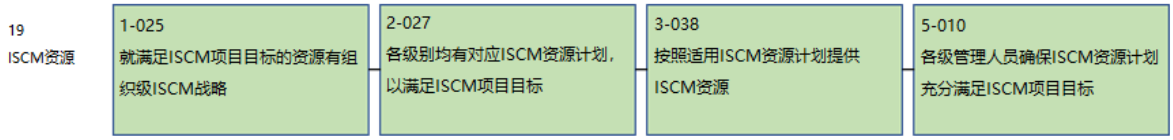

图 27：ISCM 资源追溯链

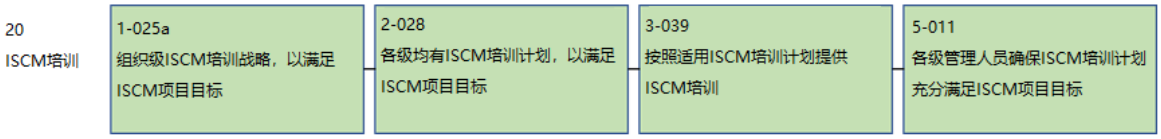

图 28：ISCM 培训追溯链

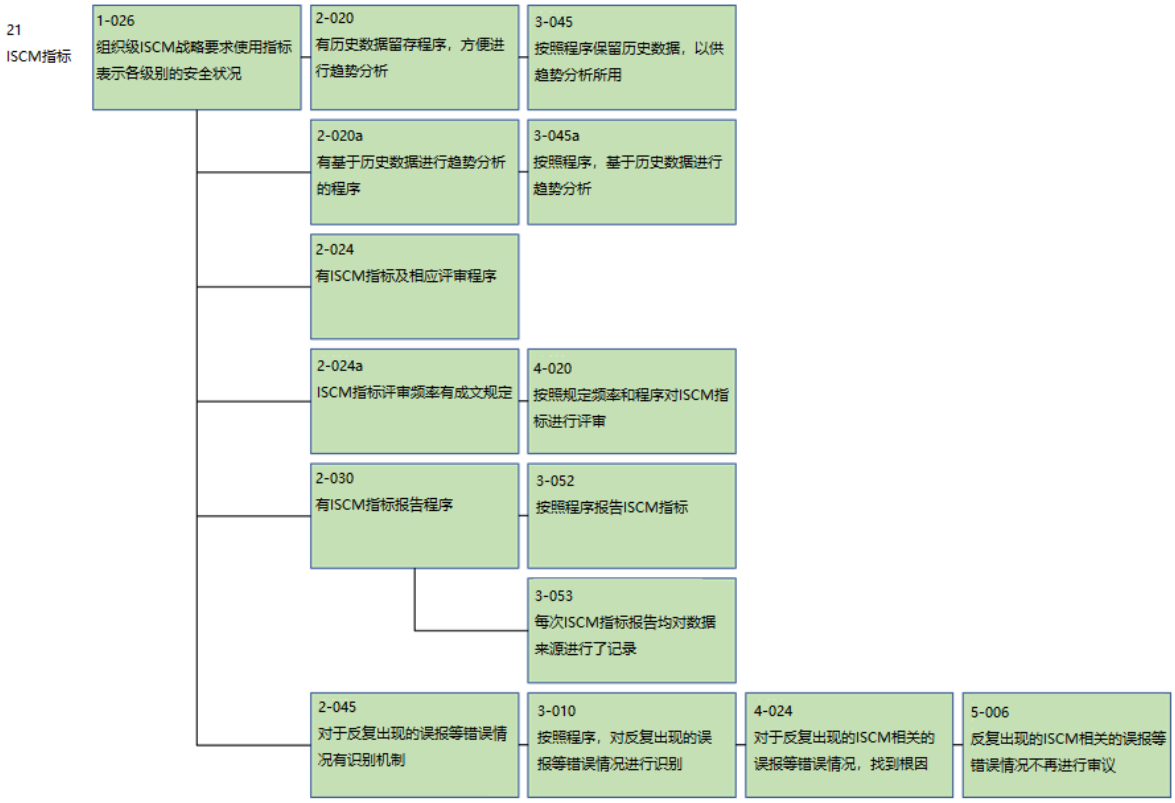

图 29：指标追溯链

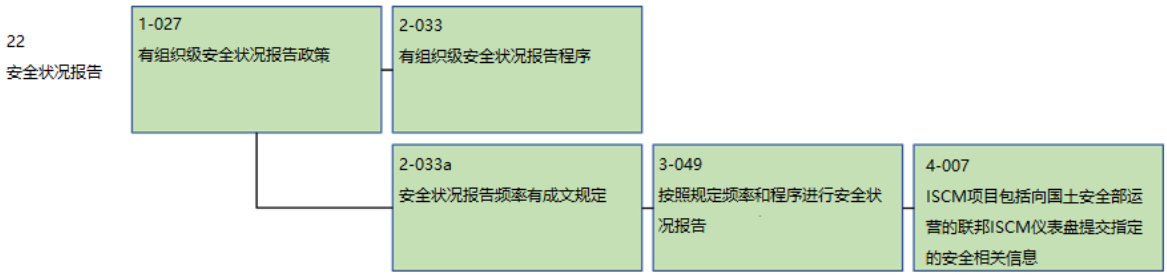

图 30：安全状况报告追溯链

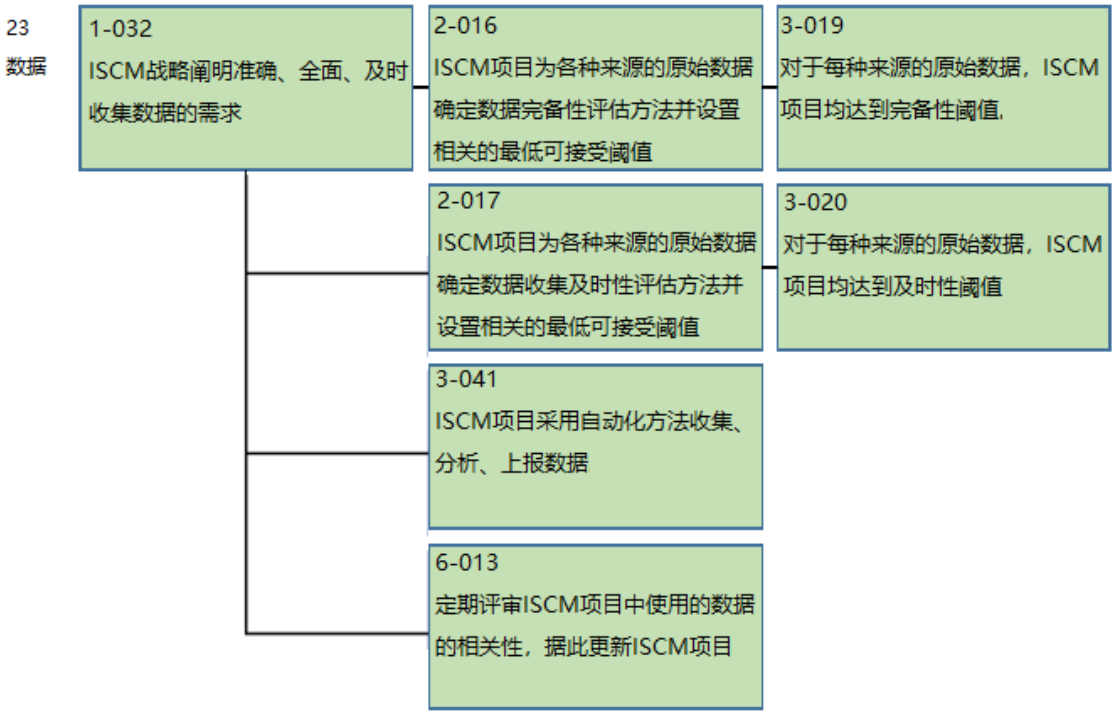

图 31：数据追溯链

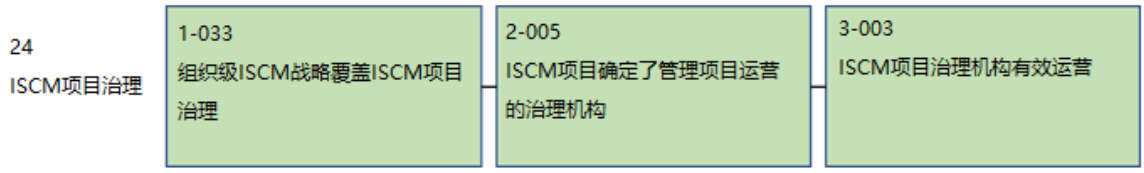

图 32：ISCM 项目治理追溯链

小蜜蜂翻译公益译文项目，旨在分享国外先进网络安全理念、规划、框架、技术标准与实践，将网络安全战略性文档翻译为中文，为网络安全从业人员提供参考，促进国内安全组织在相关方面的思考和交流。

“安全加”社区

小蜜蜂公益翻译组