安全加社区

公益翻译项目

2016

联邦信息系统和组织信息安全持续监控（ISCM）

美国国家标准与技术研究院

2011 年 9 月

文档信息			
原文名称	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations		
原文作者	Kelley Dempsey, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay	原文发布日期	2011 年 9 月

	Jones, Angela Orebaugh, Matthew Scholl, Kevin Stine		
作者简介			
原文发布单位	National Institute of Standards and Technology		
原文出处	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf		
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

计算机系统技术报告

国家标准与技术研究院的信息技术实验室旨在通过对国家的测量和标准相关的基础架构提供技术领导来促进国家经济和公共福利。ITL 设计测试和测试方法，并提供参考数据、概念验证（POC）和技术分析来推动信息技术的发展和应用。ITL 的职责包括制定技术、物理、行政及管理方面的标准和指南，实现经济高效的安全并保护联邦计算机系统中非机密的敏感信息。该报告介绍了 ITL 在计算机安全方面的研究、指导和外展活动以及与业界、政府和各学术机构之间的协作活动。

NIST SP800-137，80 页（2011 年 9 月）

本文中可能提到的商业实体、设备或资料，仅为准确描述程序或概念之目的，并非暗示 NIST 推荐或者认可，也并不意味着这些实体、资料或设备是实现目的的最佳选择。

致谢

本文作者分别有来自 NIST 的 Kelley Dempsey、Arnold Johnson、Matthew Scholl 和 Kevin Stine，美国国防部首席信息官 Ronald Johnston，来自博思艾伦咨询公司的 Alicia Clay Jones 和 Angela Orebaugh，以及来自普华永道（PwC）的 Nirali Shah Chawla。他们衷心感谢评审文档初稿和对技术内容做出贡献的同事们，对同事们在整个文档开发过程中就技术问题提供的热情帮助及独到见解，表示感谢！最后，对公共部门和私营部门的组织和个人做出的贡献，一并表示感谢。他们的深思熟虑和建设性意见，帮助提高了刊物的整体质量和可用性。

摘要

在目前情况下，组织的绝大多数的关键业务职能依赖于信息技术，管理这项技术以及确保信息的保密性、完整性和可用性对于业务来说也是非常关键的。在设计企业架构及其安全架构时，组织需要满足其治理架构、使命和核心业务过程在 IT 基础设施方面的安全需求。信息安全是一个动态的过程，必须进行有效主动的管理以识别、应对新的漏洞、不断变化的威胁，以及组织持续变化的系统架构和运行环境。

由 NIST[1]开发的风险管理框架（RMF）提供了将信息安全和风险管理活动整合于系统开发生命周期的严格、结构化的流程。持续监控是风险管理流程中的关键部分。另外，组织也应该监控其整体安全架构及其相关的安全项目，以确保即使在发生各种变化的情况下，组织仍在整体上运行于可接受的风险水平之内。及时、相关、准确的信息至关重要，机构必须有所取舍，在资源缺乏时尤其如此。

> 信息安全持续监控是指对组织的信息安全、漏洞和威胁进行持续监控，为其风险管理决策提供支持。

在组织实施任何信息安全持续监控工作或流程（process）之前，管理层必须事先对 ISCM 策略（strategy）进行全面定义，该战略涵盖技术、流程、规程（procedure）、运行环境和人的因素。该策略：

- 基于对组织的风险容忍度的明确了解，帮助管理人员为整个组织设定优先级和管理风险；
- 提供相关指标，以衡量组织各层级的安全状况；
- 确保安全控制措施的持续有效性；
- 验证是否符合信息安全要求，符合组织的任务/业务职能、联邦法律、法令、规定、政策和标准/指南；
- 考虑到组织所有的 IT 资产，如实反映其安全状况；
- 确保了解并控制组织系统和运营环境的变化；以及
- 对威胁和漏洞保持关注。

[1] 见 NIST 特别刊物（SP）800-37（修订版），《关于在联邦信息系统中应用风险管理框架的指南：安全生命周期方法》。

ISCM 立项后，按照预先制定的指标收集信息，在此过程中所参考的部分信息通过实施安全控制措施获得。组织的管理人员按需定期收集分析数据，并根据各组织层级的需要管理风险。这个过程涉及到整个组织的各级人员，从负责公司治理和战略规划的高级领导到各种组织核心任务/业务流程支撑系统的具体开发、实施和操作人员。这样就可以从组织全局的角度对风险缓解、拒绝、转移和接受活动进行有效决策。

组织的安全架构、安全运行能力、监控流程会随着时间的推移不断改进和成熟，以更好地应对动态的威胁和漏洞局面。应根据需要，定期审核组织 ISCM 策略和项目的相关性，对其进行必要调整，提高对资产可见性以及对漏洞的了解，同时对组织的信息基础架构实施数据驱动控制，并提升组织的抗打击能力。

组织范围的监控难以仅凭手工流程或自动化流程有效达成。使用手动流程时，过程是可重复、可验证的，能够持续实施。自动化流程（包括使用自动化支持工具如漏洞扫描工具和网络扫描设备）使持续监控活动更有效、更具有成本效益和一致性。在 NIST SP 800-53，《联邦政府信息系统推荐使用的安全控制措施（修订版）》中定义的许多技术性安全控制措施是监控活动中自动化工具和技术的优先选项。通过使用自动化工具对技术控制措施进行实时监控可以让组织动态了解这些控制措施的有效性及组织的安全状况。重要的是，所有综合的信息安全项目，均须对所实施的安全控制措施（包括管理和操作性控制措施）定期进行有效性评估，即使相关监控无法或很难自动化。

组织通过采取以下步骤建立、实施和维护连续监控项目。这些步骤包括以下内容：

- **定义** ISCM 策略；
- **建立** ISCM 项目；
- **实施** ISCM 项目；
- **分析**数据并**报告**发现；
- 对发现做出**响应**；以及
- **评审和更新** ISCM 策略和项目。

健康的 ISCM 项目能够使组织从合规驱动的风险管理转向数据驱动的风险管理，为组织提供必要的信息，为风险应对决策、安全状况信息和持续了解安全控制有效性提供支持。

1.0 概述

信息安全持续监控（ISCM）是指对组织的信息安全、漏洞和威胁进行持续监控，为其风险管理决策提供支持[2]。根据组织风险容忍度，本文特别强调对安全控制有效性、组织安全状态的评估和分析。安全控制有效性体现在实施的正确性以及根据当前的风险容忍度，控制措施满足组织需求的程度（比如，控制措施是否符合安全计划，并能处理威胁？安全计划是否充分？）[3]。通过组织确立的安全指标衡量组织的安全状态，了解组织信息和信息系统的安全状况，并根据已知威胁信息了解组织的抗打击能力。因此，以下内容将成为必需：

- 保持对组织范围内所有系统的态势感知；
- 持续了解威胁和威胁活动；
- 评估所有的安全控制措施；
- 收集、关联并分析安全相关信息；
- 在组织各层级间传达可靠的安全状况信息；和
- 组织管理人员主动进行风险管理

在制定策略及执行项目过程中，与所有利益相关主体的沟通非常关键。本文采用了 NIST SP 800-37《联邦信息系统应用风险管理框架指南：安全生命周期方法（第一版）》中介绍的监控概念。虽然不时有不可避免的变化，ISCM 项目能够保证部署的安全控制措施持续有效，并且运行保持在组织可接受的风险水平内。如果确认安全控制措施不足，ISCM 项目可根据风险程度协助制定优先安全响应措施。

只有在更广泛的组织需求、目标或战略情景下，ISCM 策略才有意义，可视为更广泛的风险管理战略不可或缺的一部分，及时管理、评估和响应不断涌现的安全问题。通过 ISCM 项目收集的信息支持连续授权决策[4]。

作为组织风险管理框架（RMF）关键的一步，通过 ISCM 项目，组织人员可按需访问安全相关信息，及时做出风险管理决策，包括授权决策。还可以经常更新安全计划、安全评估报告、行动计划与里程碑、硬件和软件清单和其他系统信息。如果可能的话，部署自动化机制进行数据收集和报告，此时 ISCM 项目效果最为显著。统一输出格式，提供特定、可测量、可操作、相关、及时的信息，可进一步提高有效性。尽管本文鼓励使用自动化，但是 ISCM 项目的诸多方面是难以实现自动化的。

1.1 背景

监控信息系统安全的概念早已被公认是完善的管理实践。1997 年，美国行政管理和预算局（OMB）的 A-130 通告附录 III[5]中要求组织审核其信息系统安全控制措施，确保系统变化不会严重影响安全，安全计划持续有效，并且安全控制措施能够按计划进行。

2002 年的《联邦信息安全管理法案》（FISMA）进一步强调了连续监控信息系统安全的重要性，要求组织根据风险定期评估安全控制措施，至少每年一次。

最近，OMB 发布了 M-11-33 备忘录《2011 财年联邦信息安全管理法案及机构隐私管理的报告要求》[6]。备忘录提供了 FISMA 年报说明，并强调要持续监控信息系统的安全状态从而做出持续的风险决策。

---

[2] 注意，这里的“持续”是指定期对安全控制措施和组织风险进行评估和分析，且该频率足以为组织进行基于风险的安全决策提供支持，可对其信息进行充分保护。无论频率如何，都要在不连续时间间隔内进行数据收集。

[3] NIST SP 800-53A（修订版）对安全控制有效性的定义是：“在多大程度上，能够正确执行控制措施、按预期运行和达到理想的结果，从而符合系统的安全要求”。

[4] 关于持续授权信息，参见 OMB 备忘录 M-11-33，问题 28（http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf）。

[5] 了解 OMB 通告 A-130，参见 http://www.whitehouse.gov/omb/circulars_a130_a130trans4。

[6] 了解 OMB 备忘录 M-11-33，参见 http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf。

能够对信息系统的某些方面进行自动监控的工具已成为数据获取和数据分析的有效手段。各厂商所提供产品的易用性、可用性和广泛的适用性能够保证监控工具的快速部署，支持做出接近实时的风险决策。

1.2 与其他特刊的关系

NIST SP 800-39《管理信息安全风险：组织、任务和信息系统》描述了三项关键的组织 ISCM 活动：有效性监控、系统与运营环境变化监控、合规性监控。NIST SP 800-37 描述了系统级别的安全控制措施（见 RMF 步骤 6）、提供了组织视角，融合系统开发生命周期（SDLC）和支持持续性授权。进一步深化了 NIST SP 800-39 和 NIST SP 800-37 中的概念，为制定 ISCM 策略和执行 ISCM 项目提供充分指导。

NIST SP 800-37 与 NIST SP 800-39 介绍了分层方法：1 层是组织，2 层是任务/业务流程，3 层是信息系统。在 NIST SP 800-39 中，这些层级用于从不同的组织视角进行风险管理。本文借用层级的概念来定义不同层级的 ISCM 任务。针对组织层、任务/业务流程层和信息系统层，提供各层 ISCM 指导方案（ISCM policy）、规程和职责。尽可能使用自动化。在自动化不切实际或不可能时，采用手动（比如程序化的）监控方法。

随着时间的推移 ISCM 项目将不断演化，可利用额外工具和资源，测量和自动化功能日益成熟，做一些改变以持续改进组织的安全状态和安全项目。定期审核监控策略的相关性，判断其是否准确反映了组织的风险容忍度、测量的正确性、衡量指标的适用性，以及支持风险管理决策的有效性。

1.3 目的

该指南旨在帮助组织制定 ISCM 策略，实施 ISCM 项目，提供威胁和漏洞感知，提高组织资产的可见性和安全控制措施的有效性。ISCM 策略和项目能够持续保证计划和执行的安全控制措施与组织的风险容忍度相匹配，并确保能够及时提供风险响应所需要的信息。

1.4 目标受众

本文服务于与联邦信息系统的设计、开发、实施、运行、维护和处理相关的关人员，包括：

- 任务/业务负责人或受托人（例如：联邦机构负责人、首席执行官和首席财务官）
- 负责开发和集成信息系统的人员（例如：项目经理、信息技术产品开发人员、信息系统开发人员、信息系统集成商、企业架构师和信息安全架构师）
- 负责信息系统和/或安全管理/监督的人员（例如：高级主管、风险主管、授权主管、首席信息官和高级信息安全主管）
- 负责信息系统、安全控制评估和监控的人员（例如：系统评估人、审核人/审核小组、独立的验证评估人、审计师或信息系统负责人）；以及
- 负责信息安全实施和运营的人员（例如：信息系统责任人、通用控制措施提供人、信息负责人/管理人、任务/业务负责人、信息安全架构师和信息系统安全工程师/管理人[7]）

1.5 内容简介

本文其他章节内容如下：

- 第 2 章介绍持续监控信息安全支持风险管理的基本原理；
- 第 3 章介绍 ISCM 流程，包括实施指南；以及

附录介绍了 ISCM 的补充信息，包括：（A）参考文件、（B）术语定义、（C）缩略语和（D）实施 ISCM 所需技术。

[7] 在*机构层*，该职位也被称为高级机构信息安全主管。在组织内，该职位也叫做首席信息安全官。

2.0 基本原理–持续监控对风险管理的支持

本章介绍了在组织范围内持续监控信息安全的基本概念，以及如何应用 ISCM 项目支持组织风险管理决策（例如风险应对决策、持续性系统授权决策、《行动计划和里程碑》（POA&M）资源和优先级决策等）。为了有效应对日益加剧的安全挑战，精心设计的 ISCM 策略用以评估安全控制措施有效性，并监控安全状况[8]，采用的流程能够确保响应措施与评估结论和组织的风险容忍度相匹配，并保证响应能达到预期效果。

第 3 章中介绍了 ISCM 项目的实施流程，如下：

- **定义** ISCM 策略；
- **建立** ISCM 项目；
- **实施** ISCM 项目；
- **分析**数据并**报告**发现；
- 对发现做出**响应**；和
- **评审和更新** ISCM 策略和项目。

ISCM 策略随着风险决策和信息需求的发展而发展。这些需求可能来自组织的任何层级。组织根据内部安全状况持续控制负责人的要求来实施 ISCM 项目，将风险控制在可接受范围内。实施项目时，全组织应尽量使用标准化方法，以通过最少的资源（例如：工具/应用采购资金、数据调用、组织范围内的政策/规程/模板等）来最大化利用安全相关信息。分析数据为管理管理组织的安全态势和整体风险的不连续流程提供信息。根据收集的资源信息（如人、流程、技术和环境），ISCM 使组织可了解组织的系统安全状态的态势感知，有能力应对情况变化。

在组织范围内的宏观风险管理战略[9]中，ISCM 项目是一项战术。组织通过增强监控能力来提高态势感知能力，从而进一步洞察和控制管理组织安全的流程。反过来，洞察和控制安全流程又能促进态势感知。因此，ISCM 项目的实施流程是递归的。ISCM 与组织的各种安全流程及安全相关信息的输入输出需求互为参考，并输入和输出安全相关信息。例如：

与系统组件清单存相关的安全信息用来确定《CM-8 信息系统组件清单》[10]的合规性，从而评估控制措施是否有效（比如，清单信息是否正确）。如果清单信息不正确，则开始分析导致信息不正确的根本原因（比如，可能是组件联网流程被忽略或已过时，资产管理工具不能正常运行，或者组织被攻击等原因）。根据分析结果，酌情响应（比如，责任方更新清单、更新相关组织流程、开展员工培训或断开问题设备等）。除此之外，与系统组件清单相关的安全信息还可用于支持预定义的衡量指标。正确的系统组件清单能够提高其他安全域（如补丁管理和漏洞管理）的有效性。

这个例子说明了如何利用在评估安全控制措施过程中收集的数据来计算指标，并为各种组织流程提供输入。还进一步说明了一旦一个问题被检测到，它可以触发对组织一项或多项控制措施的评估，对相关的安全信息的更新，对组织的安全项目和安全流程的修改，并促使组织更好地遵循安全项目和适用的系统安全计划。最终结果是组织范围内的风险管理和持续改进得到改善，不过具体的时间表取决于组织收集信息的速度和对发现结果的响应速度。

2.1 组织的 ISCM 观

在组织层面保持信息安全风险的实时沟通绝非易事，需要多方努力。这项工作涉及到整个组织的各级人员，从负责公司治理和战略规划的高级领导到支持组织核心任务与业务功能的信息系统的开发、实施和操作人员。图 2-1 说明了如何在组织内分层实施 ISCM，以支撑风险管理。1 层涉及治理、风险管理目标和组织风险容忍，这些都会推动 ISCM 策略的制定。

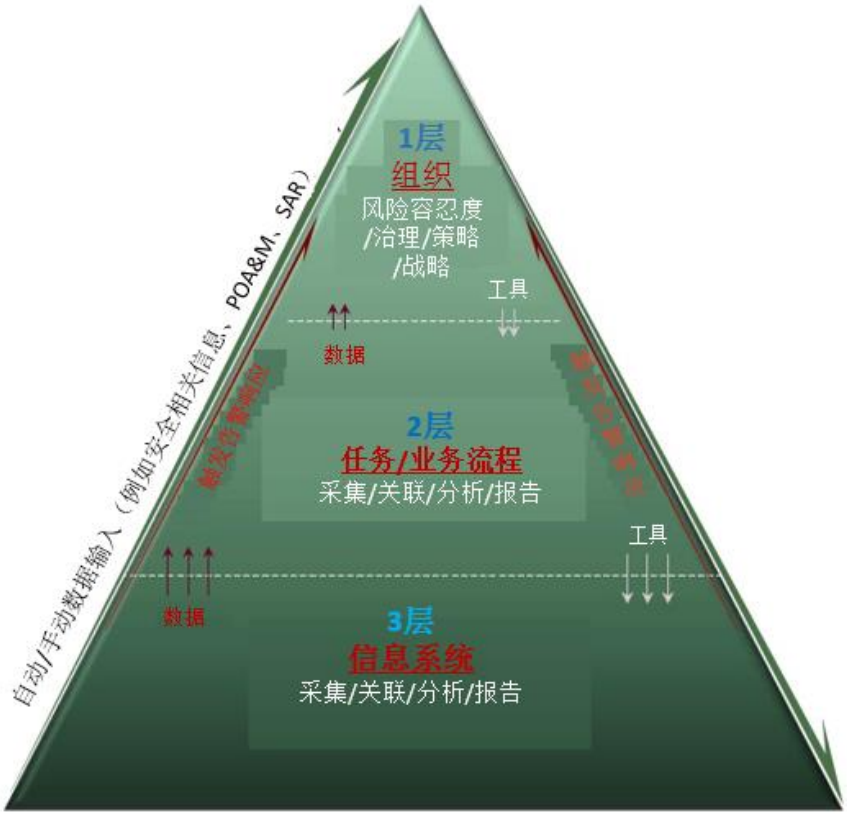
---

[8] 组织执行管理组织安全和衡量指标的流程，通过指标能够了解这些流程和组织安全状况。一些安全流程与安全控制措施保持一致，其他安全流程则与控制措施的组件或组合保持一致。关于衡量指标，参见 NIST SP 800-55（修订版）《信息安全绩效评测指南》的第 3.2.1 节。

[9] NIST SP 800-39，在讨论组织范围内的风险管理时介绍了 ISCM。

[10] CM-8 是配置管理族中的一项安全控制措施，参见 NIST SP 800-53 中的附录 F。

进行风险管理（功能）[11]的高级主管/领导所制定的组织风险容忍度将会影响各层的 ISCM 指导方案、规程和实施活动。数据收集主要发生在信息系统层。衡量指标根据各层具体情况分别制定。例如，在 3 层收集的 ISCM 数据可提供单个系统、多个系统、核心业务流程或整个组织的安全状态或风险评分。可在任意层制定策略、规程和工具。然后，在 1 层或 2 层制定时，有助于在组织范围内保证实施的一致性，更有效地支持数据复用和资源合理利用。数据收集、分析和报告等应尽量自动化[12]。与手动流程相比，通过自动化，可监控更多的安全指标，同时使用更少的资源、更多的样本[13]，实现更高的频率、更好的一致性和可靠性。组织可定期审核 ISCM 策略，确保指标持续相关、有效、可靠，可为组织管理人员进行风险管理决策提供支持。



组织持续监控信息和信息系统安全的方法支持组织层（1 层）、任务/业务流程层（2 层）和信息安全层（3 层）的风险相关决策[14]。

2.1.1　1 层—组织

1 层风险管理活动是针对高级信息安全治理政策，因为它与整个组织、核心任务和业务功能的风险息息相关。在 1 层，ISCM 项目的标准是由组织的风险管理战略来定义的，包括组织计划如何评估、响应和监控风险，以及如何监督，确保风险管理战略的有效性。管理人员在 1 层定义的安全控制措施、安全状态和其他衡量指标，都是为了为风险管理决策提供必要信息，以利于管理。制定 1 层是为了支持治理决策，事关组织、核心任务和业务功能。可根据从通用、混合和具体的系统安全控制措施中获得的安全相关信息计算 1 层指标。指标与监控[15]报告的频率应按需制定，保证组织运营在可接受的风险容忍范围内。作为组织整个管理架构的一部分，1 层风险管理策略和相关监控要求在 2 层和 3 层依然有效。

---

[11] 关于风险主管（功能）的角色和职责，参见第 2.4 节。

[12] 在确定如何最佳利用从单个信息系统收集的安全相关信息来计算组织的安全和风险指标时，务必小心。仪表盘和指标可提供组织安全和风险的态势感知，但是如果未确认指标相关性就使用，会导致对安全的错误认识。

[13] 如果组织不具有在信息基础设施内对每一个相关对象进行评估所必需的资源或基础设施，采样是一项可减少持续监控工作的有效方法。详细信息参见第 3.1.4 节。

[14] NIST SP 800-39（修订版）提供了风险管理的整体方法。

[15] 本文中，组织指标监控也被称为安全状况监控。

2.1.2 2 层–任务/业务流程

管理人员负责一项或多项任务或业务流程，并负责监督这些流程的相关风险管理。2 层信息安全持续监控标准的制定取决于以下因素：（1）对于组织的整体目标与短期目标而言，核心任务/业务流程的优先级；（2）成功执行既定任务/业务流程所需的信息类别；（3）组织范围内的信息安全项目战略。项目群管理（PM）家族的控制措施属于 2 层安全控制措施。这些控制措施强调，组织信息安全项目 2 层控制措施的建立和管理应在全组织内部署，并支持所有信息系统。可在 2 层或 1 层跟踪这些安全控制措施。在某种程度上，2 层安全控制的评估频率以及安全状态和其他指标的监控频率或多或少取决于目标、任务或业务流程的优先级、基础设施固有的测量能力[16]。安全相关信息可能来自通用、混合和系统特定的控制措施。在 1 层和 2 层，指标和仪表板用于评估、标准化、沟通和关联监控活动中。这些活动是在任务/业务流程层下进行的。

2.1.3 3 层–信息系统

3 层 ISCM 活动从信息安全角度进行风险管理。这些活动包括确保所有系统级的安全控制措施（技术、操作和管理控制措施）的正确实施、按需操作、产生预期结果，从而满足对于系统的安全要求，并随着时间的推移继续有效。3 层 ISCM 活动还包括评估和监控在系统级实施的混合和通用控制措施。通常，在该层的安全状态报告包括但不限于安全告警、安全事件和已识别的威胁活动[17]。3 层的 ISCM 策略还能确保安全相关信息支持组织其他层的监控要求。系统级控制措施（系统特定的、混合的、或通用的控制措施）的数据源/评估结果，以及相关的安全状态报告，都支持在组织和任务/业务流程层的基于风险的决策。信息根据每层需求定制，并为各层决策提供数据支持。那些决策影响应用在信息系统层的 ISCM 策略[18]。源于信息系统层的 ISCM 指标可用于评估、响应和监控整个组织的风险。在信息系统层执行的持续监控活动为授权主管（AO）提供安全相关信息，支持其做出持续性的系统授权决策，并为风险主管（功能）提供安全相关信息，支持持续性的组织风险管理。

在 3 层，RMF 步骤 6 监控活动和 ISCM 活动协调一致。对已执行的安全控制措施的评估方法是相同的，区别在于正在进行的评估仅支持系统授权，还是支持更广泛的、更全面的持续监控工作。信息系统层主管和员工进行评估和监控，并持续分析结果。组织层、任务/业务流程层和信息系统层都利用信息支持风险管理。尽管频率要求不尽相同，每层都能接收到适用于受影响流程的当前安全相关信息。在 ISCM 项目环境中执行的 RMF 步骤 6 活动支持风险和接受，比如持续授权（RMF 步骤 5）。

2.2 持续系统授权

初始授权操作是基于某一个时间点的证据，但系统和运行环境是不断变化的。对安全控制有效性的持续评估，支持在随时间推移而高度动态的操作环境中进行系统的安全授权。这样的操作环境中充满了不断变化的威胁、漏洞、技术和任务/业务流程。通过 ISCM，可及时评估新的威胁或漏洞信息，因此组织可根据需要调整安全要求或个别控制措施，维护授权决策。系统授权获取流程即风险管理框架（RMF）[19]，多数情况下是为了管理信息安全与信息系统相关的风险。RMF 是一个提供了一个严谨的、结构化的流程，将信息系统安全和风险管理活动融入 SDLC，如图 2-2 所示。RMF 的监控步骤（步骤 6）包括图 2-1 中所示的 ISCM 组织层级之间的互动。这种互动涉及系统负责人、通用控制措施提供人及授权主管向风险主管（职能）[20]提供安全控制评估数据以及系统和通用控制措施持续授权等数据，还包括由 1、2 层向授权主管和信息系统负责人传递风险更新信息（如漏洞和威胁数据）及组织风险容忍度信息。当 RMF 应用于一个已执行健康的 ISCM 策略的组织时，组织管理人员将获得组织安全状态的信息，以及按需提供各系统对整体安全态势的影响。

---

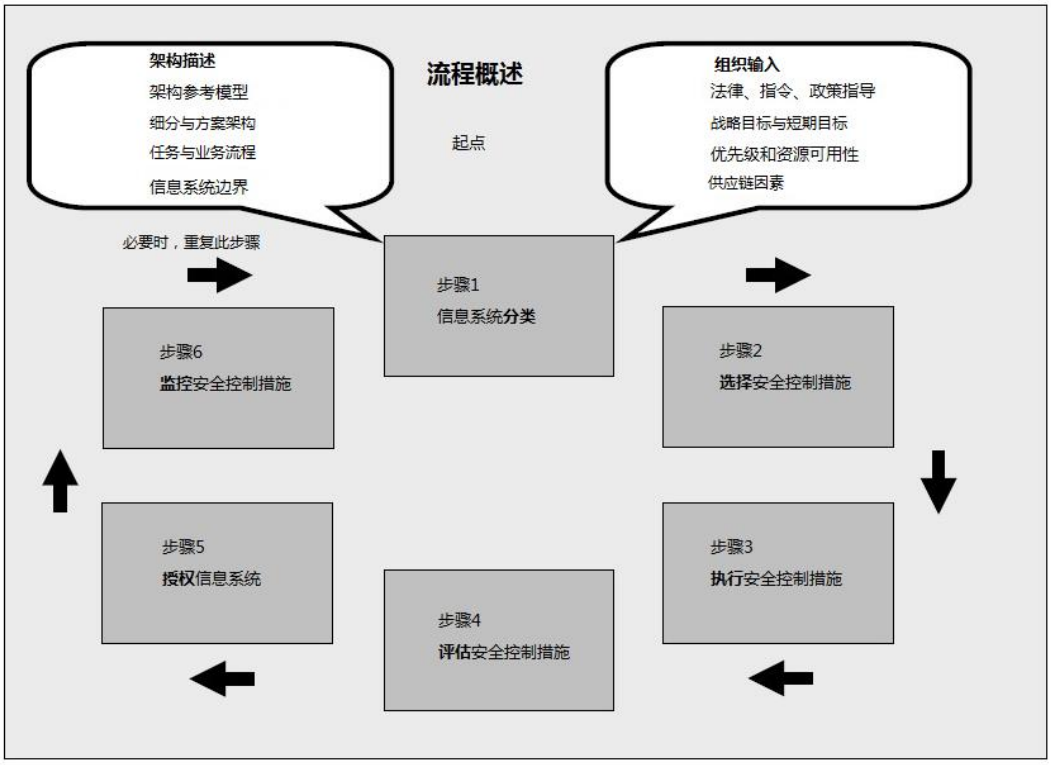
16 随着组织技术和人力资本能力的日渐成熟，监控能力也有所增长。

17 威胁活动包括在组织网络中的恶意活动或异常行为。关于更多威胁信息，参见 NIST SP 800-30（修订版）。

18 某一系统的持续监控策略可能还包括对其他系统造成潜在影响的相关指标。

19 在一定程度上，系统操作授权部分依赖于对通用控制措施的评估/监控与持续安全授权。NIST SP 800-37 修订版描述了对通用控制措施的安全授权。

20 关于持续监控项目中的人员角色和职责，参见第 2.4 节。NIST SP 800-37（修订版）描述了风险主管（功能）在 RMF 中的交互。



管理良好的组织范围内的战略性 ISCM 项目的输出可用于支撑系统授权，保证所需的系统信息和数据（例如《系统安全规划与风险评估报告》、《安全评估报告》和 POA&M）是最新的。安全管理和报告工具还能提供对关键证据自动更新的功能，支持持续性授权决策。ISCM 可推动对持续授权的风险决策，通过按需提供不断变化的威胁活动或漏洞信息，理信息系统，对通用控制措施进行安全授权。这样，安全控制评估和风险判断流程就由静态授权转化为一个动态的过程，支持及时的风险响应措施和高效的持续授权。对威胁、漏洞和安全控制措施有效性的持续监控，为基于风险支持持续授权提供了态势感知信息支持提供态势感知。一个设计合理的 ISCM 策略和项目支持的持续授权类型有：单一授权、联合授权和杠杆式授权[21]。

支持持续评估和授权的 ISCM 可能是资源密集的和费时的。收集安全相关信息并随时评估部署在组织内的每项安全控制措施的方方面面，是不切实际的。更为可行的方法是设定一个合理的评估频率，收集安全相关信息。评估频率根据系统分类与 ISCM 策略要求确定，应足以保证与风险相匹配的安全水平。对信息系统安全对象进行采样，而不是 100%检查，也是一项有效的监控手段，特别是在非自动化监控的情况下。第 3 章将讨论在确定采样规模和监控时需要考虑的重要因素。

监控频率（例如，每年、每季度、每月或每天）并非一成不变，会因衡量指标不同而不同。例如，可以调整安全控制评估和监控频率，以应对组织信息系统或其运行环境的变化，包括安全威胁和漏洞的新信息。在响应安全事件中，ISCM 优先级应不断变化和调整，以确认安全控制实施的问题或评估对安全有重大影响的系统和系统组件的变化。ISCM 策略可提供关于安全相关数据的动态更新，支持随时进行系统授权。第 3.2.2 节详细讨论了在确定监控频率时需要考虑的因素。

2.3 ISCM 中的自动化

组织一般尽量寻求自动化解决方案，以降低成本、提高效率和提高安全相关信息监控的可靠性。安全是通过人、流程和技术共同实现的。信息安全自动化主要涉及的是只需很少人机交互的安全自动化。自动化工具往往能够识别分析师可能不会注意的模式和关系，特别是

[21] 关于授权类型，参见 NIST SP 800-37（修订版）。

对大量数据进行分析时。这包括验证单个网络端点上的技术设置或确保机器上安装的软件符合组织的最新策略。自动化有助于推进组织内的安全流程，并能减少人力重复劳动，使训练有素的专业人员把时间放到需要人类认知的任务上。

ISCM 策略不仅仅关注组织容易收集或容易自动化的安全相关信息。ISCM 项目在初次实施时，组织安全项目的多个方面可能需要手动监控。随着时间的推移，组织的监控能力将逐步扩展和趋于成熟。结合经验教训和对组织安全状况及风险容忍度的深入了解，衡量指标也将不断演变。ISCM 策略的焦点是提供足够的关于安全控制有效性和组织安全状况的信息，使组织人员能够做出明智、及时的安全风险管理决策。因此，所有安全控制措施的实施、有效性和充分性，以及组织安全状况，都受到监控。

在确定组织 ISCM 自动化程度时，组织应考虑自动化对流程标准化的潜在促进，并从风险管理的角度考虑自动化安全相关信息的潜在价值（或价值缺失）。并且，组织还应考虑无形资产，比如人员分配的潜在价值和更全面的态势感知。

虽然 IT 安全自动化能够显著减少必须花费在做某些任务上的人力时间，却不可能将组织信息安全项目的功能完全自动化。例如，附录 D 中的技术仍要求“人”对工具的实现和维护进行分析，以及对发现结果的恰当诠释。同样地，这些工具是在人为设计、运行和维护的环境下运行的。如果个人不能安全地履行职责，那么技术的有效性就会受到影响，并且系统安全和系统所支持的任务/业务或组织流程都将岌岌可危。

有了自动化，即使持续监控需求不断变化，获取安全相关信息也易如反掌。因此，在安全控制措施的实施（RMF 步骤 3）过程中，要考虑到现有技术支持 ISCM 的能力，以确定实施特定控制措施的最佳方案。

应考虑以下 ISCM 工具：

- 从各个来源（例如：评估对象[22]）获取信息的工具；
- 使用公共规格（比如安全内容自动化协议（SCAP））的工具；
- 提供与其他产品（例如帮助台、库存管理、配置管理和事件响应解决方案）互通的工具；
- 遵守适用的联邦法律、行政命令、指令、政策、法规、标准和指南的工具；
- 提供报表功能，报表应可定制输出格式，覆盖高级、汇总及系统级指标；以及
- 允许数据合并到安全信息和事件管理（SIEM）工具和仪表盘产品中的工具。

2.4 角色及职责

本节介绍在组织 ISCM 项目中主要参与者的角色及职责。不同的任务和组织结构可能导致对 ISCM 相关的角色命名和在组织人员的具体职责分配方面有所不同（例如，多人共同承担一个角色或一人充当多个角色）。通常，ISCM 的角色和职责包括：

代理负责人。代理负责人很可能和风险主管（职能）一起参加组织的 ISCM 项目。

风险主管（职能）。风险主管（职能）监督组织的 ISCM 策略和项目。风险主管（职能）审核从 ISCM 流程中获取的状态报告，作为信息安全风险状况和风险容忍度决策的输入信息，为任务/业务流程与信息系统层实体提供 ISCM 策略与需求方面的输入；促进组织实体间的协同合作及安全相关信息共享；在组织范围内讨论所有的风险源；确保进行持续监控决策时考虑了风险信息。

首席信息官（CIO）。CIO 领导组织的 ISCM 项目。CIO 对组织 ISCM 项目提出期望和要求，确保组织建立有效的 ISCM 项目并付诸实施；与授权主管密切合作，为 ISCM 提供资金、人力和其他资源支持；维护高层交流和组织实体之间的工作组关系。

高级信息安全官（SISO）。SISO 建立、实施和维护组织的 ISCM 项目；对安全项目和信息系统的持续监控进行指导（例如，指导方案/规程）；为组织提供配置管理指导；巩固和分析 POA&M，判断组织的安全漏洞与不足；获得/开发并维护支持 ISCM 和持续授权的自动化工具；提供关于组织 ISCM 项目和流程的培训；为信息主管/信息系统主管和通用控制措施

[22] 关于更多评估对象信息，参见 NIST SP 800-53A（修订版）。

提供人提供在各自信息系统实施 ISCM 方面的支持。

授权主管（AO）。AO 负责 ISCM 项目在特定信息系统中的应用。AO 确保维护信息系统的安全状态得以维护，审核安全状态报告和重要的安全文档，判断信息系统运行所带来的风险是否还在组织的接受范围内。AO 还判断信息系统发生重大变化时是否需要重新授权。如果需要，AO 对信息系统进行重新授权。

信息系统负责人（ISO）/信息主管/管理人。ISO 为组织 ISCM 项目在系统层的执行制定流程和规程。这包括为信息系统开发和记录 ISCM 策略；参与组织的配置管理流程；建立和维护与信息系统相关的组件清单；对信息系统的变化进行安全影响分析；根据 ISCM 策略对安全控制措施进行或确保其得到评估；根据组织政策和规程，编制和提交安全状况报告；按需进行修复，维护系统授权；按需修改系统级的安全监控流程；审核通用控制措施提供人的 ISCM 报告，从而验证通用控制措施能够继续为信息系统提供足够的保护；根据 ISCM 结果，更新关键的安全文档。

通用控制措施提供人[23]。通用控制措施提供人建立流程和规程，支持对通用控制措施的持续性监控。通用控制措施提供人为指定的通用控制措施制定和记录 ISCM 策略；参与组织的配置管理流程；建立和维护与通用控制措施相关的部件清单；分析对通用控制措施变化的安全影响；确保根据 ISCM 策略评估安全控制措施；根据组织政策/规程，编制和提交安全状态报告；必要时，进行缓解活动，维护通用控制授权；按需更新/修改通用安全监控流程；发生变化时，更新关键的安全文档；根据组织政策/规程，将关键的安全文档分发给信息责任人/信息系统责任人和其他高级主管。

信息系统安全官（ISSO）。ISSO 通过协助 ISO 完成 ISCM 职责和参与配置管理流程的方式，来支持组织 ISCM 项目。

安全控制评估人。安全控制评估人为 ISCM 项目中收集到的安全相关信息分类，并为组织 ISCM 项目评估信息系统或项目管理安全控制措施。安全控制评估人为每一项安全控制措施制定安全评估规划；在评估前，提交安全评估规划进行审批；按照安全评估规划，评估安全控制措施；在 ISCM 发生变化时，更新安全评估报告；在必要时，更新/修改安全评估规划。

组织可能会按需定义其他角色（例如，信息系统管理员和 ISCM 项目主管）以支持 ISCM 流程。

[23] 组织可能有多个通用控制措施提供人。

3.0 流程–定义 ISCM 策略和执行 ISCM 项目

本章描述制定 ISCM 策略和执行 ISCM 项目的流程，包括在组织层、任务/业务流程层和信息系统层的各种活动。设计合理的 ISCM 策略包括安全控制评估、安全状况监控和安全状况报告，支持全组织做出及时的风险决策。ISCM 策略还会融入流程，确保能够采取响应措施。基于收集的数据制定组织行动策略和收集数据一样重要（如果说前者没有后者更重要的话）。制定 ISCM 策略和实施 ISCM 项目的流程如下：

- 根据风险容忍度，**定义** ISCM 策略，保持对资产、漏洞、最新威胁信息和任务/业务影响有清晰的认识。
- **建立** ISCM 项目，确定衡量指标、状态监控频率、控制评估频率和 ISCM 技术架构。
- **制定** ISCM 项目，收集安全相关信息，用于衡量指标、评估和报告。在可能的情况下自动化数据收集、分析及上报。
- 分析收集的数据和上报发现，确定适当的响应措施。有必要收集额外的信息，以澄清或补充现有的监控数据。
- 开展技术、管理和操作性的缓解活动来响应评估结果，或接受、转移/共享、避免/拒绝调查结果。
- 审核和更新监控程序，从而调整 ISCM 策略和完善测量能力，提高对资产的可见性和漏洞感知，进一步启用组织的信息基础设施的安全数据驱动控制，提高组织的抗击打能力。

ISCM 流程如图 3-1 所示。

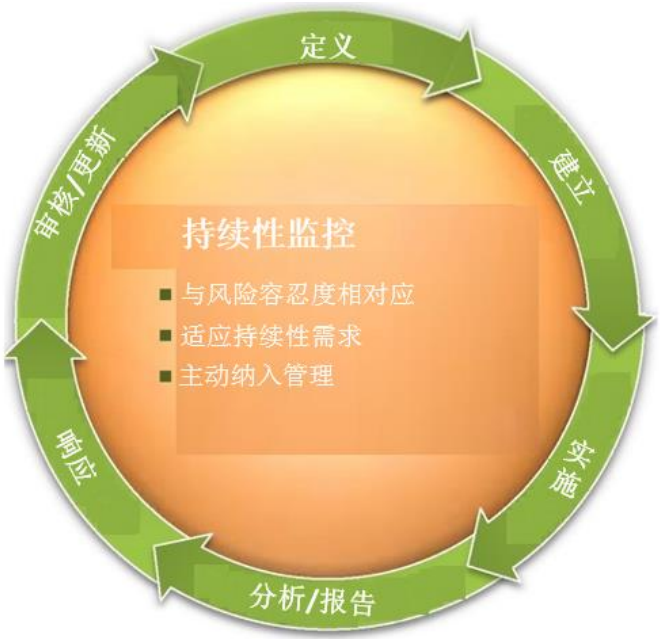


图 3-1 ISCM 流程

风险容忍度、企业架构、安全架构、安全配置、对企业架构的变更计划以及可用的威胁信息提供数据，这些数据是执行这些步骤和对安全相关的风险进行持续管理的基础。分析安全相关信息，因为它与各层的组织风险管理均相关。

本章其他部分讨论了 ISCM 流程，详细介绍现有指南中未涉及的话题，并恰当引用了现有指南。主要角色、次要角色、预期输入和输出为每个流程步骤提供指导。角色和责任在不同的组织中不尽相同，ISCM 项目的实现细节亦如此。

3.1 定义 ISCM 策略

要有效实施 ISCM，首先要制定战略，ISCM 要求和在各组织层级（组织层、任务/业务流程层和信息系统层）的活动。每层按照既定的频率监控安全指标和评估安全控制的有效性，定制状态报告，以支持各层的决策。在 1、2 层执行的策略、规程、工具和模板，或按照

在 1、2 层的指南进行管理的策略、规程、工具和模板，能够最好地支持层内和层间的数据共享。根据组织架构，每层的任务和活动可能会有所重叠。

下述准则尽管非指令性要求，但有助于确保在组织范围内的 ISCM 方法能够最好地提升标准化的方法和一贯实践，从而最大程度地提高效率，充分利用安全相关数据。因为变化时有发生，需要审核 ISCM 策略的相关性和准确性，以反映组织的风险容忍度、措施的正确性和衡量指标的适用性。任何 ISCM 策略都包括标准（描述了策略审核或更新的触发条件），还要审计预先设定的评估频率。同样，组织根据修改后的 ISCM 策略定义更新 ISCM 项目的标准和规程。

3.1.1 组织（1 层）和任务/业务流程（2 层）的 ISCM 策略

风险主管（功能）判断整体的组织风险容忍度和组织层[24]的风险缓解战略。制定和执行 ISCM 策略，以支持按照组织的风险容忍度进行风险管理。尽管可以在任何层制定 ISCM 策略、策略和规程，组织范围内的 ISCM 策略及相关政策是在组织层制定的，而一般执行规程是在任务/业务流程层制定的。如果组织范围内的战略是在任务/业务流程层制定的，1 层主管审核和批准该战略，以确保在所有任务和业务流程中都适当考虑到组织的风险容忍度。此信息传达给任务/业务流程和信息系统层的员工，并在任务/业务流程和信息系统层的战略、策略和规程中反映出来。

当在 1 层和/或 2 层制定下面的这些策略、规程和模板时，它们能够促进组织范围内的标准化流程，支持 ISCM 策略。

- 定义关键指标的策略；
- 用于修改和维护监控战略的策略；
- 评估安全评估措施（包括通用、混合和系统级的控制措施）有效性的策略和规程；
- 用户安全状态监控的指导方案和规程；
- （关于控制有效性和状态监控的）安全状况报告的指导方案和规程；
- 评估风险和获取威胁信息和见解的指导方案和规程；
- 用于配置管理和安全影响分析的指导方案和规程[25]；
- 执行和使用组织工具的指导方案和规程；
- 确定监控频率的指导方案和规程；
- 确定样本大小和总体以及管理对象采样的指导方案和规程；
- 确定安全指标和数据源的指导方案和规程；
- 风险评估模板；以及
- （关于控制有效性和状态监控的）安全状况报告的模板。

策略、规程和模板强调手动和自动的监控方法。组织在这些层制定指导方案和规程，对 ISCM 角色的人员进行培训，包括如何管理和使用自动化工具（比如，建立基线和调整衡量方法，从而对运营环境进行恰当的监控），还可包括如何识别风险超限触发条件并恰当响应相关告警，以及对内部或外部报告要求的培训。这样的培训可能包括在针对重要安全角色的培训要求，或者仅针对组织实施者，进行组织 ISCM 指导方案和规程执行方面的培训。

当上层执行指导方案、规程和模板时，下层会填补与该层流程相关的空白。1 层和 2 层的决策和活动可能会受到以下约束：任务/业务需求、基础设施（包括人文因素）的局限性、僵化的管理策略和外部驱动因素。

主要角色：风险主管（职能）、首席信息官、高级信息安全官及授权主管

次要角色：信息系统负责人/通用控制措施提供人

[24] 关于风险主管（功能）的角色和职责，参见 NIST SP 800-39（修订版）。
[25] 关于更多安全配置管理信息，参见 NIST SP 800-128（修订版）。

期望输入：组织风险评估和当前风险容忍度、当前威胁信息、组织期望和优先级、OMB 业务线和/或第三方厂商提供的工具

期望输出：关于组织风险容忍度、组织范围内的 ISCM 策略和相关策略、规程、模板和工具的更新信息

3.1.2 信息系统（3 层）ISCM 策略

为支撑风险管理，系统级 ISCM 策略的制订与实施不仅须在信息系统层级进行，还应该根据系统与组织的风险容忍度贯穿*所有三个层级*。虽然该策略可在 1、2 层定义，针对各系统的实施指导方案与规程在 3 层制定也未尝不可。系统级安全相关信息包括系统级安全控制评估数据以及从系统级安全控制措施获取的指标数据。系统负责人创建系统级 ISCM 策略时考虑的因素包括系统架构与运行环境、组织与任务需求[26]、指导方案、规程与模板。

系统级 ISCM 旨在监测安全控制措施是否有效（评估）、监测安全状况以及汇报结论。各种安全控制措施（包括在系统层面实施的通用与混合控制措施）最起码应按照系统安全计划及 NIST SP 800-53A 文件（修订版）规定的方法进行有效性评估。系统负责人基于各层的驱动因素确定安全控制措施的评估频率，相关信息，详见 3.2.2 节。系统级安全相关信息用于确定各层的安全状况，相关信息，详见 3.2.1 节。

信息系统层的 ISCM 策略还支持持续授权。所谓持续授权，指根据评估与监控频率持续更新授权决策信息。对组织层面或任务/业务流程层面实施并管理的通用控制措施进行监控并形成评估结果，这些结果可与信息系统层产生的信息结合，为授权主管进行授权提供客观全面的证据支持[27]。ISCM 获取的评估证据至少应按组织指导方案要求的频率提供给授权主管。

主要角色：信息系统负责人/通用控制措施提供人、信息系统安全主管

次要角色：高级信息安全主管、授权主管、安全控制评估人

期望输入：组织风险容忍度信息、组织 ISCM 策略、指导方案、规程、模板、系统威胁信息、系统信息（如《系统安全计划》、《安全评估报告》、《行动计划与里程碑》、《安全评估计划》、《系统风险评估》等[28]）

期望输出：系统级 ISCM 策略，这是对 1、2 层策略及组织安全项目的补充，为各层级提供安全状况信息，并按照组织 ISCM 策略要求实时更新持续系统授权决策。

3.1.3 流程角色及职责

1、2 层管理人员在整个 ISCM 流程中的职责包括但不限于如下各项：

- 为组织 ISCM 策略的制订提供输入，包括制订指标、指导方案、规程，编制 3 层数据并将其与 1、2 层所用安全相关信息进行关联，拟定评估及监控频率指导方案，提出使用采样法所需遵循的深度与广度要求【ISCM 步骤：定义、制订、实施】；
- 评审监控结果（安全相关信息），根据组织指导方案及定义判断安全状况【ISCM 步骤：分析/汇报】；
- 分析信息系统及其运行环境的变化对组织及任务/业务流程功能的潜在安全影响，以及新增、移除信息系统对企业架构的安全影响【ISCM 步骤：分析/汇报】；
- 确定现有风险是否在组织风险可容忍范围内【ISCM 步骤：分析/汇报、评审/更新】；
- 根据持续监控活动及风险评估结果，采取必要行动（如请求制订或修改指标、新增或调整评估方法、修改现有通用或项目群管理安全控制措施、新增控制措施）应对风险

[26] 设计 ISCM 策略时，其中一个目的是确保对于安全架构的破坏可以得到控制，以防止该等破坏对业务及任务功能造成影响或将此种影响降至最低。

[27] 有关评估人独立性要求的具体信息，见 NIST SP 800-53，CA-2，《控制加固 1》。评估人仅须独立于系统运营，可来自组织层面、任务/业务层面或组织内外部的其他独立机构。系统操作员所给的评估结果若得到独立评估人的认定亦可使用。

[28] 该系统信息为风险管理框架输出。电子标准模板及文档管理系统可根据持续监控计划产生的数据持续更新。

【ISCM 步骤：响应】；

- 更新相关安全文档【ISCM 步骤：响应】；
- 评审新增或修订法规、指令、指导方案等中与安全要求相关的变化【ISCM 步骤：评审/更新】；
- 评审监控结果，确定是否应调整或更新组织计划及指导方案【ISCM 步骤：评审/更新】；
- 评审监控结果，确定新增漏洞信息【ISCM 步骤：评审/更新】；
- 评审如下信息中所暴露的新威胁：监控结果、威胁建模（基于资产与攻击）、分类与未分类威胁摘要、USCERT 报告及通过可信来源、跨部门分享及外部政府来源获得的其他信息【ISCM 步骤：评审/更新】。

3 层管理人员在整个 ISCM 流程中的职责包括但不限于如下各项：

- 为制订、实施组织范围内的 ISCM 策略以及制订、实施系统级 ISCM 策略提供输入【ISCM 步骤：定义、制订、实施；RMF 步骤：选择】；
- 支持安全控制措施的规划与实施、自动化工具的部署以及为实施 ISCM 策略而进行的不同工具的连通【ISCM 步骤：实施；RMF 步骤：选择】；
- 判断信息系统及其运行环境的变化（包括与系统试运行或停运相关的变化）带来的安全影响【ISCM 步骤：分析/汇报；RMF 步骤：监控】；
- 评估持续安全控制的效果【ISCM 步骤：实施；RMF 步骤：评估[29]、监控】；
- 根据持续监控活动结果、风险评估、行动计划与里程碑未决项目采取必要行动（如请求新增或调整评估方法、修改现有安全控制措施、实施新增的安全控制措施、接受风险等）应对风险【ISCM 步骤：响应；RMF 步骤：监控】；
- 基于 ISCM 流程结果，为安全计划、安全评估报告以及行动计划与里程碑提供持续输入【ISCM 步骤：响应；RMF 步骤：6】；
- 汇报信息系统的安全状况，包括 1、2 层指标的输入数据【ISCM 步骤：分析/汇报；RMF 步骤：评估、监控】；
- 评审汇报的信息系统安全状况，确定对系统及组织带来的风险是否在组织风险可容忍范围【ISCM 步骤：分析/汇报；RMF 步骤：授权、监控】。

3.1.4 定义样本总体

组织会发现从组织内各系统的所有对象收集数据可能不够现实，成本也太高昂。这时，可使用采样方法，这种方法对于手动和自动监控均适用，可提升 ISCM 的成本效益。不过，采样也有风险，因为它无法像总体评估那样覆盖所有对象，捕捉所有的结果差异，因而可能无法准确反映安全控制的有效性及组织安全状况。

针对三种指定的评估方法（检视、面谈、测试），NIST SP 800-53A 文件（修订版）中介绍了如何确定样本总体以保证恰当的覆盖度。NIST SP 800-53A 文件围绕基本、专门、综合[30]三种测试方法，对于“代表性评估对象样本”或“足够大的评估对象样本规模”提出了指导意见。可使用统计工具来确定样本规模。

NIST 800-53A 文件为解决一般性采样问题及样本覆盖度提供了指导意见。在确定样本总体时，从如下三个方面保证足够的覆盖度：

- **对象类型**：保证评估对象种类足够丰富；

[29] 初始授权前，系统未包含在组织的持续监控项目中。系统在运行后才与 RMF4 相关，然后通过步骤 4 支持持续授权。

[30] 见 NIST SP 800-53A（修订版）附录 D。

- **每种对象的数量：**每种类型应选择“足够多”的对象，以确保评估额外对象时结果一致；
- **每种类型的特定评估对象：**若组织内所有相关对象均可评估，样本总体中的每种类型数量应“足够多”，以充分应对评估结果中的已知或预期方差。

样本的测量结果用统计量（如样本均值）表示，观测值与容许值之间的差异即组织的风险容忍度。若样本总体非随机选择以及样本规模（即测试对象数量）较小，用采样法获得的统计结果也许不够可靠[31]。NIST 的《工程统计学手册》中提到，在确定样本总体应包含的对象数量时，应虑及如下因素[32]：

- 想要获得的信息（通过测评可解决什么问题）
- 评估成本与效用
- 对象、组织或运行环境的已知信息
- 样本总体的预期变异性
- 统计结果的目的置信度以及与样本总体相关的结论

在全组织内“提升”或“进一步提升控制措施正确执行及正常运行的置信度”有以下方法：提出更多有针对性的问题、增加评估对象类型、增加每种评估对象的数量。

组织还可以将上述标准用于具体的评估对象而不仅仅是随机样本。不过，非随机采样应谨慎使用，以避免偏性。自动化数据采集与分析可以减少采样需求。

主要角色：信息系统负责人、通用控制措施提供人、信息系统安全主管、安全控制评估人

次要角色：风险主管（职能）、授权主管、首席信息官、高级信息安全主管

期望输入：ISCM 策略相关的组织及系统级指导方案与规程、指标、按评估与监控频率更新的《安全评估计划》

期望输出：《安全评估计划》中的可接受样本规模文档、安全相关信息

3.2 建立 ISCM 项目

组织需建立 ISCM 策略实施项目。该项目应能够为风险决策提供参考，能维持风险容忍范围内的正常运营。要实现的目标包括检测组织的运营及信息系统环境中的异常与变化、洞悉资产情况、感知漏洞、了解威胁、确认安全控制有效性以及安全状况（包括合规性）。设计指标，确定频率，提供必要信息，将风险控制在组织的风险容忍范围内。在设计架构内采用工具、技术及手动和/或自动方法，在恰当范围内以恰当频率分发要求的信息。

3.2.1 确定指标

组织需确定指标，以评估、控制组织内的持续性风险。指标包括所有安全相关信息，这些信息或从评估中获得，或由自动或手动监控获得。指标提供的信息应条理清晰、意义明确，可满足决策及汇报要求。指标应基于与维持或提升安全状况相关的具体的目标。针对系统级数据制订指标可辅助任务/业务或组织的风险管理。

指标会用到不定期采集的安全相关信息，因此数据延迟会有不同。计算指标时可基于安全状况监控及安全控制评估数据，还可基于从一个或多个安全控制措施采集的数据。可为某一层级或整个组织设立指标，如发现与修复的漏洞数量和严重性、非法访问次数、配置基线信息、应急方案测试日期及结果、了解风险意识培训要求的员工数量、组织风险容忍度阈值、与特定系统配置相关的风险值。

例如，组织用以监控合法与非法网络组件状态的指标可能依赖于如下相关指标：实物资产位置、虚拟资产位置（子网/IP 地址等）、MAC 地址、系统关联、网络连接指导方案/规程。指

[31] 中心极限定理是一个重要定理，允许人们假设由随机样本计算的统计量（如均值）呈正态分布（如钟形曲线），无论样本个体的母体如何分布。对于小样本量（约少于 30），正态分布假设仅在随机样本的母体分布接近正态时才有效。

[32] 有关确定样本量的详细信息，见 http://www.itl.nist.gov/div898/handbook/ppc/section3/ppc333.htm。

标根据 ISCM 策略不定期更新，可按小时、按天或按星期计算。虽然虚拟资产信息每天都会有变化，网络连接指导方案及规程最多一年评审或调整一次。这些指标并非是推荐指标，仅为参考之用，之所以提及，是为了便于理解跨层级指标的概念。每个组织应根据实际情况定义指标及相关监控频率。计算指标时，应根据指标的时间要求定期评估与监控相关的控制措施或措施及其对象。

应注意的是，指标本质上是有缺陷的，无法保证正确执行*所有的*安全控制措施。定义或计算指标时应基于安全架构的输出。若安全架构中的安全控制措施未经过评估，基于这样的架构采集指标则无异于使用一杆破烂或不准的秤来称重。对于指标数据的解读应基于这样的假设：指标计算中直接、间接使用的控制措施均正常实施并运行。指标表明有问题存在的话，根因会有多种。有些安全控制措施与指标*无关*，在无法从根本上保证这些措施被正确执行并持续有效的情况下，根因分析无法顺畅进行，分析会局限于预先拟制的清单，而忽视了真正的问题。制订指标的相关信息，详见 NIST SP 800-55 文件（修订版）。

主要角色：风险主管（职能）、首席信息官、高级信息安全主管

次要角色：授权主管、信息系统负责人/通用控制措施提供人

期望输入：组织风险评估、组织风险容忍度、现有威胁信息、汇报要求、现有漏洞信息

期望输出：既定指标，它们可以反映各层的安全状况及安全控制有效性，为报表接收方/用户直观展示资产，使其了解漏洞及威胁所在。

3.2.2 确定监控及评估频率

组织 ISCM 项目的关键功能之一是确定安全状况监控及安全控制评估的频率。对有些组织来说，仪表盘及持续评估与既有的完整安全控制评估模式不同，这类评估多在明确的时间点进行。组织若规定了*每个*安全控制措施或控制元素的有效性评估频率及*每个*指标的监控频率，则这种转变对于安全、保障和资源利用会具有积极有效的推动作用。

单一层级或整个组织范围的安全控制有效性本身可作为安全指标，具有相关的状况监控频率。虽然每个指标与控制措施都有自己的监控与评估频率，组织仍会使用具有不同时延的数据来反映所有系统的整体安全状况和企业架构安全状况。随着监控项目的成熟，监控与评估频率对于数据的使用方法将会具有重要意义，“*系统何时可授权运行*”这个问题变得没有“*系统弹性如何*”这个问题更有意义。

确定评估与监控频率需考虑的因素

组织在确定指标监控频率或安全控制评估频率时需考虑如下因素：

安全控制的易变性。不管是为了安全控制的有效性还是为了支撑指标的计算[33]，易变的安全控制措施都要求更高的评估频率。NIST SP 800-53 配置管理（CM）系列针对的就是易变的控制措施。信息系统配置一般变动会很频繁，系统配置中未授权或未分析的变动常会使系统面临被攻击的风险。因此，如 CM-6 配置设置及 CM-8 信息系统部件清单之类的相关控制措施需要频繁的评估与监控。这种评估与监控最好使用 SCAP 验证的自动化工具，以根据需要提供报警及状态信息。相反，如 PS-2 职位分类或 PS-3 人员筛选（属于 NIST SP 800-53 人员安全系列）之类的控制措施在多数组织设置中比较稳定，会在相当长的一段时间内保持静态，因此一般不需要频繁评估。

系统分类/影响级别。通常，安全控制措施的监控频率与相关系统的受影响程度（高、中、低）相关，系统受到的影响越大，安全控制措施的监控频率就越高[34]。

- **提供关键功能的安全控制措施或评估对象。**提供关键安全功能的安全控制措施或评估对象（如日志管理服务器、防火墙等）也需要较频繁地监控。此外，支持关键安全功能并/或被认为对系统（基于业务影响分析[35]判断）或组织有关键作用的个别评估对象要求的评估频率也会较高。

- **确认具有漏洞的安全控制措施。**安全评估报告中记录的已知风险需要频繁监控，将其

[33] 安全控制的易变性衡量的是控制措施在实施后动态变化的频率。

[34] 这里系统影响程度的含义与 FIPS 199 及 NIST SP800-60 所述一致。

[35] 见 NIST SP 800-34 修订版《联邦信息系统应急计划指南》，2010 年 5 月。

控制在可容忍范围之内。同样，《行动计划与里程牌》中记录的有漏洞的控制措施也需要频繁监控，直到漏洞修复。注意，并非所有的漏洞都要求相同的监控频率。例如，安全评估报告里定义为对系统或组织有轻微或低级影响的漏洞，其监控频率就不必像高影响漏洞那么高。

- **组织风险容忍度[36]。**风险容忍度低的组织（如处理、存储或传输大量私有及/或个人验证信息的组织、有大量高影响系统的组织、面临特定持续性威胁的组织）监控频率高，而具有较高风险容忍度的组织（如极少使用中、低影响系统来处理、存储或传输个人验证信息及/或私有信息）监控频率则较低。

- **威胁信息。**组织在确定监控频率时需考虑现有可信威胁信息，包括已知利用漏洞及攻击模式[37]。例如，若利用已实现技术中的漏洞发动攻击，可暂时或长期提升对于相关控制措施或指标的监控频率，防护此种威胁。

- **漏洞信息[38]。**组织在确定监控频率时应考虑与 IT 产品相关的现有漏洞信息。例如，若某一特定产品厂商每月提供一次软件补丁，组织可考虑至少以相同频率进行漏洞扫描。

- **风险评估结果。**在确定监控频率时，应检视及考虑组织及/或系统的（正式或非正式）风险评估结果。例如，若系统风险评估中发现了与非本地维护（NIST SP 800-53，MA-4）相关的威胁和漏洞，组织要考虑更频繁地监控非本地维护与诊断活动记录。若组织已有风险评分方案，可参考风险分值提升或降低相关控制措施的监控频率。

- **监控策略评审输出。**3.6 节详述了如何评审与调整监控策略。

- **汇报要求。**汇报要求不会驱动 ISCM 策略，但对监控频率有影响。例如，若行政管理和预算局（OMB）指导方案要求每季度上报检测到的非法组件数量及所采取的纠正措施，组织应至少按季度监控系统中的非法组件。

组织按已确定频率获取要求的数据，并据此部署人力与物力。随着自动化能力或资源的不断增加，组织可考虑提升受影响控制措施及指标的监控频率。同样，若可用资源减少，组织可考虑相应调整监控频率，这样，一方面保证安全相关信息得到适度分析，另一方面又满足了组织对于风险进行持续管理的要求。

NIST SP 800-53 目录中的许多安全控制措施及控制加固措施有多重实施要求。针对同一个控制措施，具体的控制要求及/或控制加固措施会以不同频率评估或监控。例如，AC-2 账户管理针对基准控制有 10 条要求（a~j），另外还有 4 项控制加固措施【（1）~（4）】。根据上述考虑因素，每条要求对应不同的监控频率。例如，AC-2a 涉及的是账户类型识别，在一个典型的信息系统中，账户类型在被识别或记录后很少再有变化。因此，AC-2a 的评估频率较低。AC-2h 涉及的是去激活临时账户及已终止或调动用户的账户。组织一般会有频繁的人员变动，因而评估 AC-2h 的频率会比 AC-2a 的频率高。AC-2（3）要求，系统应自动停用指定时间内处于非活跃状态的账户。这是一个自动化控制措施，具有典型的高易变性，因而监控频率应较高，同时可自动化某些基准控制要求，按照组织的 ISCM 策略使其接受更频繁地监控。

组织与任务/业务流程层级

在任务/业务流程层，组织确定每一安全控制措施或指标的最低评估或监控频率。组织内的所有系统及通用控制措施都应基于本节上述标准确定评估频率。通用、混合及系统安全控制措施受制于组织及任务/业务流程层的指导方案与规程。许多组织系统会继承使用通用控制措施，这类措施的总体重要性要求更高的评估频率，而只负责保护单一系统的控制措施的评估频率会相对较低。此外，确定通用控制措施的评估频率时，组织还需要判断通用控制措施提供人的可信度。与流程相关的通用控制措施（如规程/模板、项目群管理控制等）不会频繁变动，自动化程度不高。这种情况下，组织在确定评估频率时仍应考虑这些措施及其相关威胁信息的易变性。

主要角色：首席信息官、高级信息安全主管

---

[36] 确定组织风险容忍度的详细信息，见 NIST SP 800-39（修订版）。

[37] 攻击模式基于对特定现实攻击所作的深度分析,描述了利用软件的常用方法。详细信息，登录 http://capec.mitre.org/，查阅《常见攻击模式枚举与分类（CAPEC）》。

[38] 现有漏洞信息可在 http://www.kb.cert.org/vuls 及 http://nvd.nist.gov/中查阅。

次要角色：风险主管（职能）、授权主管、通用控制措施提供人、信息系统负责人

期望输入：组织风险评估、组织风险容忍度、现有威胁信息、汇报要求、现有漏洞信息、监控策略评审输出

期望输出：组织指导方案及规程、每个安全控制措施及指标的推荐评估及监控频率

信息系统层

在信息系统层，系统负责人评审组织及/或任务/业务流程层指导方案所确立的最低监控/评估频率，确定这个最低频率对于某一特定信息系统是否恰当。对于某些信息系统，可能须评估是否提升组织规定的个别控制措施或指标的评估频率，这个评估仍要基于本节上述标准。系统负责人还要考虑识别哪些系统组件应比其他系统组件（如对外服务器、边界防护设备、业务影响分析中确定的关键组件等）进行更频繁地评估。

主要角色：信息系统负责人、信息系统安全主管

次要角色：授权主管、高级信息安全主管、信息主管/管理人

期望输入：确定了最低频率的组织策略与规程、现有威胁信息、汇报要求、现有漏洞信息、策略评审监控输出、安全评估计划

期望输出：按系统安全控制措施的评估频率以及指标的监控频率定期更新的安全评估计划

事件驱动的评估

事件发生后，可能会要求立即进行安全控制措施的评估或安全状况的验证，即使 ISCM 策略中未有相关要求。这种情况下的评估未经规划，但是 ISCM 策略中定义了其类型，或者经过定制，可满足突发需求（如更改已确立评估或监控频率）。例如，若在系统中新增了一个 Web 应用，包含配置管理与控制、安全影响分析、开发漏洞扫描等的现有 ISCM 流程便足以对该新增 Web 应用进行评估。

在定义事件驱动评估的标准时，组织会考虑如下因素：安全事件、新威胁信息、系统与运行环境的主要变化、新增或额外的任务职责、安全影响分析或风险评估结果。

根据事件的重要性，事件驱动的评估会触发一个或多个系统重授权。

主要角色：信息系统负责人/通用控制措施提供人、授权主管、信息系统安全主管

次要角色：风险主管（职能）、高级信息安全主管、安全控制评估人

期望输入：组织风险评估、组织风险容忍度、现有威胁信息、现有漏洞信息、组织优先考虑的事项及期望

期望输出：事件驱动评估/授权的标准与阈值文件（如重大更改规程、事件驱动授权指导方案与规程）

3.2.3 建立 ISCM 架构

组织确定如何在层级内及层级间、组织外采集与传递信息。ISCM 实施架构的核心要求包括数据采集、数据存储、数据分析能力以及检索与展示（汇报）能力。方法需要标准化以提升效率，促进层级内及层级间的信息交流、关联及其他分析。

组织恰当使用自动化工具、技术与方法以提升效率，洞悉从各方收集、分析并传播的大量数据。架构及其相关指导方案与规程的设计目的是最大程度地减少数据调用，尽可能地增加数据复用[39]。数据输入来源各不相同（如授权包、培训记录、系统日志），满足不同利益主体的要求。数据规范的互通（如 SCAP 和 XML）保证数据在采集后可以多次复用。安全状况各方面工作由组织内不同角色或职能完成，因此要求在不同的指标与环境中按不同的频率使用原始数据（如安全评估与授权、用户意识与培训、访问控制等）。同样，组织的任务及业务功能对于汇报的要求不同，采取行动的原因也各不相同（如风险容忍度的变化、运行环境的变化（包

[39] ISCM 架构样例见 NISTIR 7756 草案《CAESARS 框架扩展：企业持续监控技术参考架构（草案）》。

括不断变化的威胁活动）、安全架构调整、安全状况汇报等）。

3.3 执行 ISCM 计划

ISCM 应按策略执行。根据需要收集安全相关信息（数据），满足预定义指标的要求，进行安全控制评估，根据组织指导方案与规程汇报生成的安全相关信息。组织的持续监控项目定义了*所有的*安全控制类（管理、运营与技术）及类型（通用、混合与系统）。每种控制措施都要监控其有效性，都会在安全状况监控时用到。数据源包括人、流程、技术、计算环境及现有相关安全控制评估报告。

尽可能自动化数据采集、分析及上报。数据在手动或自动采集后被集中起来供分析所用，并被上报至组织内负责关联与分析风险管理活动数据的员工。如上面各例所述，这可能意味着在不同的时间点从多种来源获取数据，并按多种方式组合成有意义的数据，按要求提供给上述负责人。

在持续监控流程中实施阶段的部分环节，ISCM 数据按决策要求被有效整理并传递给利益相关主体。组织的 ISCM 架构要求选择恰当的工具与方法，以确保风险决策基于准确无误的安全相关信息。

不连续安全流程与 ISCM 数据互为参考。ISCM 数据还可以用来为那些非信息安全风险控制流程提供参考。同样，这些流程中的数据也可以作为 ISCM 项目的参考。与 ISCM 互为参考的流程包括但不限于补丁管理、资产管理、许可证管理、配置管理、漏洞管理与系统授权。

如第二章中所述，某一流程的 ISCM 数据输出可作为其他流程的输入。

主要角色：信息系统负责人、通用控制程序提供人、信息系统安全主管、安全控制评估人

次要角色：风险主管（职能）、授权主管、首席信息官、高级信息安全主管

期望输入：ISCM 策略相关的组织及系统级指导方案与规程、指标、按评估与监控频率更新的安全评估计划、自动化规范

期望输出：安全相关信息

3.4 分析数据、汇报结果

组织制定评估与监控结果的分析、汇报规程，包括接收 ISCM 报表的具体员工/角色、汇报内容与格式、汇报频率、使用的工具。此外，对于不易自动化的控制措施，还需要分析、汇报其使用效果。某些情况下，可能需要采集额外数据来补充或解释所分析的或初始报表提供的安全相关信息。系统与任务/业务级员工按相关层级的指导方案与规程的要求接收并提供报表。

3.4.1 分析数据

组织分析 ISCM 产生的安全相关信息。某些情况下，可能需要采集额外数据来补充或说明所分析的安全相关信息。待分析信息可以连续报表、自动化报表、专门报表、数据输入或数据库视图的方式提供给组织相关负责人。

ISCM 产生的安全相关信息可从如下角度进行分析：已确定的风险容忍度、漏洞对信息系统、任务/业务流程、以及组织的潜在影响、所选择缓解方案的潜在影响。即使是实时或接近实时的组织及系统的安全相关信息，分析中也要考虑不断变化的漏洞与威胁数据。组织相关负责人评审分析后报表，以确定是否采取缓解行动或转移、避免/拒绝或接受风险。在某些情况下，授权主管可判断接受某些特定风险是否比执行缓解措施更为有利。作出这种判断应基于组织风险容忍度、对任务/业务流程的负面影响、成本效益/实施投资回报率。风险的解决与判断理由应按组织指导方案与规程进行记录。

主要角色：风险主管（职能）、首席信息官、高级信息安全主管；授权主管、安全控制评估人

次要角色：信息系统负责人、通用控制措施提供人、系统安全主管

期望输入：安全相关信息、组织 ISCM 策略、组织风险容忍度、汇报要求

期望输出：各层安全状况信息分析；更新后《系统安全计划》、《安全评估报告》、《行动计划与里程碑》；调整后组织风险管理决定

3.4.2 安全控制评估报告

组织应根据组织要求出具针对所有已实施安全控制策略的有效性评估报告。评估中的安全相关信息可以模板或电子表格形式记录，或自动采集并上报。在系统层，评估中的安全相关信息可直接支撑持续授权决策及行动计划与里程碑的制订与追踪。某些安全控制措施或安全控制措施元素被定义为安全指标（如 SI-4 信息系统监控），这样，评估这些控制措施的有效性实则为监控相关指标的安全状况。

员工应按组织指导方案与规程汇报评估结果，上级组织如行政管理和预算局（OMB）还可能要求汇报额外的指标及/或评估结果。组织在 ISCM 策略中定义安全状况汇报要求，包括接收 ISCM 报表的具体员工/角色、汇报内容与格式、汇报频率、使用的工具。

3 层管理人员上报评估结论、记录系统级缓解方案的实施并/或向 1、2 层管理人员提供建议。1、2 层组织管理人员评审 3 层管理人员的结论，确定总体安全状况，判断是否*所有控制措施*均可以充分、有效地满足任务/业务及组织的信息安全需求。报表内容因接收人、汇报频率、汇报目的、所支持的工具集以及所使用的指标的不同而不同。例如，风险主管（职能）会收到针对所有系统的年度总报表以及针对高风险系统的详细季度报表，而首席信息官与高级信息安全主管每季度则会收到针对所有系统的更细粒度的技术数据，授权主管每月会收到本人所负责系统的综合报表，计算机事件响应小组（CIRT）组长会在告警发生时收到异常报表，网管则会通过仪表盘实时审查网络活动，这些仪表盘每分钟更新一次，相关的概要指标则按天或小时更新。[40]对于变动性较大的特定控制措施或有缺陷、不合规的控制措施，组织应考虑提高汇报频率。

针对难以自动化的控制措施（如项目群管理控制措施），组织对其评估结果的汇报会提出具体要求。组织制定评估监控结果（包括手动获得的结果）的收集、汇报规程以及《行动计划与里程碑》信息管理、收集规程，用于频率确定、状况汇报及战略变更监控。

主要角色：系统负责人、通用控制程序提供人、系统安全主管、安全控制评估人

次要角色：风险主管（职能）、首席信息官、首席信息安全官、授权主管

期望输入：安全相关信息（评估结果）；组织 ISCM 指导方案与规程；授权主管、首席信息官、首席信息安全官及/或风险主管（职能）的汇报要求

期望输出：符合组织 ISCM 指导方案与规程的评估结果报告以及授权主管进行持续授权（或再授权）所要求的评估结果报告

3.4.3 安全状况监控报告

组织应制定安全状况监控报告规程。安全状况数据指对于全组织预先定义的指标进行监控所产生的数据，数据由组织内统一使用的工具（一般为通用控制措施）生成。组织内统一使用的工具可属于特定的一个或多个系统，但是生成的安全相关信息却不一定针对特定系统。

主要角色：系统负责人、通用控制程序提供人、系统安全主管、安全控制评估人

次要角色：风险主管（职能）、首席信息官、首席信息安全官、授权主管

期望输入：安全相关信息（安全状况数据）；组织 ISCM 指导方案与规程；授权主管、首席信息官、首席信息安全官及/或风险主管（职能）的汇报要求

期望输出：符合组织 ISCM 指导方案与规程的安全状况报告以及授权主管进行持续授权（或再授权）所要求的安全状况报告

[40] 这里提到的报告频率仅为说明之用。

3.5 响应评估/监控结论

分析监控获得的安全相关信息，作出恰当响应。各层级对于监控结果的响应包括缓解风险、接受风险、规避/抑制风险及分享/传递风险信息，采取哪种响应措施取决于组织的风险容忍度[41]。

响应的同时，应采取恰当的安全管理行动，如围绕安全实施配置管理项目。1 层对于结论的响应或会改变与组织治理有关的安全指导方案。这种响应受制于任务/业务需求、企业架构（包括人力构成）的局限性、固定的治理指导方案以及其他外部因素。2 层对于结论的响应包括要求提供其他安全相关信息、新增或调整指标、更改任务/业务流程或 3 层汇报要求及/或新增或调整通用控制措施。这种响应受制于组织治理指导方案与策略、任务/业务长短期目标以及组织资源与基础设施的局限性。3 层的缓解策略会立即对系统级风险产生直接影响，3 层对于结论的响应包括实施额外控制措施、调整此前实施的控制措施、终止系统操作授权、修改监控频率以及增加、细化对于安全相关信息的分析。系统级缓解措施受制于 1、2 层指导方案、要求及策略，确保对组织流程不会造成负面影响。

响应策略的实施需要时日，应在系统的《行动计划与里程碑》中具体规划实施行动。对于发现的缺陷，评估响应行动，立即执行缓解措施或在《行动计划与里程碑》中列示，其他关键系统文档应相应更新。持续监控过程中所作的响应若涉及安全控制措施的更改、加固或增加，应进行评估，以保证新增或更改的控制措施可有效实施[42]。此后，新增或更改的控制措施纳入总体持续监控策略。

主要角色：系统负责人、通用控制措施提供人、系统安全主管

次要角色：授权主管、高级信息安全主管、信息主管/管理人

期望输入：安全状况报告、评估结果报告（如《安全评估报告》）、组织与系统级风险评估、《安全评估计划》、《系统安全计划》、组织规程与模板

期望输出：风险响应决策、更新后系统安全信息（如《系统安全计划》、《行动计划与里程碑》、《安全评估报告》等）、更新后安全状况报告

3.6 评估、更新监控项目与策略

ISCM 策略与项目并非一成不变。安全控制评估、安全状况指标、监控及评估频率随组织需求的变化而变化。评审持续监控策略，保证策略可充分支持组织在可接受风险容忍度范围内正常运行，指标始终具有针对性，数据实时完备。策略评审有助于提高组织对于安全状况的认识，有效支持风险管理决策/持续授权，提升组织响应已知、最新威胁的能力。

组织制定规程，从各个方面评审、调整 ISCM 策略，包括总体策略的针对性、测评的准确性/正确性以及指标、汇报要求和监控评估频率的适用性、是否准确反映了组织风险容忍度。若收集的数据与汇报目的无关或无助于维护、提升组织的安全状况，组织会考虑中断该数据的收集以节约资源。促使监控策略变更的因素包括但不限于：

- 核心任务或业务流程发生变化
- 企业架构发生重大变化（包括新增或移除系统）
- 组织风险容忍度发生变化
- 威胁信息发生变化
- 漏洞信息发生变化
- 信息系统内部发生变化（包括分类/影响水平的变化）
- 与特定控制措施相关的《行动计划与里程碑》内容有增减
- 基于安全状况报告输出的趋势分析

41 风险响应相关信息，详见 NIST SP 800-39（修订版）。

42 安全控制措施须在测试环境里充分测试、审查、复查后才能更改。

- 新制定的联邦法律法规
- 汇报要求发生变化

相关负责人检视合并后的《行动计划与里程碑》内容，确定组织的信息系统中是否存在常见缺陷或漏洞，提出或要求相关人员提出解决方案。根据综合《行动计划与里程碑》，在公司范围内统一分配风险缓解资源，调整监控策略。还要分析安全状况报告与指标，以判断安全趋势，基于此进一步分析是否需要调整监控策略。例如，若在过去的 6 个月里，部件清单按周评估，结果表明一周之内评估对象几乎没有变化，或清单准确反映了*本周之前*所发生的变化，组织可将部件监控频率降至两周甚至一个月一次。反过来，若在过去的 6 个月里每两周审计一次，对审计结果的分析发现异常事件增多，组织则需要提高审计记录评审频率至一周一次。

组织的 ISCM 策略还会随着组织安全项目与监控能力的发展而变化。对于充分成熟的项目，组织应有标准化方法进行安全相关信息的收集与分析，作为任务与业务流程不可或缺的一部分，并尽可能自动化。这种情况下，安全项目须已成熟，可确保有充分的流程与规程保护企业架构，使其符合企业风险容忍度要求，并可收集、关联、分析、汇报相关安全指标[43]。

监控策略因为流程中步骤不断重复而持续优化，从这个意思上说，ISCM 是个递归过程。组织范围内的大规模 ISCM 应用涉及具体的任务/业务流程与系统层级活动，这些活动范围更小、更有针对性。换言之，3 层的 ISCM 输出是 1、2 层 ISCM 项目的输入。从图 2-1 所示的金字塔顶端（1 层）到底部（3 层），上层监控策略限定了下层监控项目的实现因素，下层的评断可能会促使上层监控策略的调整。ISCM 项目本身必须得到监控，与组织任务及目标、运营环境、威胁的变化保持一致。

主要角色：高级信息安全主管、授权主管、信息系统负责人/通用控制程序提供人

次要角色：风险主管（职能）、首席信息官、信息系统安全主管

期望输入：基于当前监控结果的趋势分析；组织风险容忍度信息；新制定法律、法规、汇报要求等信息；当前威胁与漏洞信息；要求的其他组织信息、自动化规范更新

期望输出：修订后 ISCM 策略或关于评审细节及策略无需修改的简要说明（基于已有评审流程）

[43] 安全指标的更多信息，见 NIST SP800-55（修订版）。

附录 A 参考文件

法规

1. 电子政府法案【包括联邦信息安全管理法案（FISMA）】（公法 107-347），2002 年 12 月

指导方案、指令、指示

1. 行政管理和预算局，A-130 通知附录 III，No.4 移交备忘录，联邦信息资源管理，2000 年 11 月
2. 美国行政管理和预算局 M-02-01 号备忘录，编制提交安全行动计划与里程碑指南，2001 年 10 月
3. 2002 年网络安全研究与开发法案

指南

1. 国家标准与技术研究院（NIST）特别刊物（SP）800-12，计算机安全介绍：NIST 手册，1995 年 10 月
2. NIST SP 800-34，第一版，联邦信息系统应急计划指南，2010 年 5 月
3. NIST SP 800-37，第一版，联邦信息系统应用风险管理框架指南：安全生命周期方法，2010 年 2 月
4. NIST SP 800-39，管理组织、任务与信息系统的信息安全风险，2011 年 3 月
5. NIST SP 800-40，第二版，创建补丁与漏洞管理项目，2005 年 11 月
6. NIST SP 800-53，第三版，联邦信息系统与组织推荐安全控制措施，2009 年 8 月
7. NIST SP 800-53A，联邦信息系统与组织安全控制措施评估指南：如何制定有效的安全评估计划，2010 年 6 月
8. NIST SP 800-55，第一版，信息安全绩效评测指南，2008 年 7 月
9. NIST SP 800-92，计算机日志管理指南，2006 年 9 月
10. NIST SP 800-126，第一版，安全内容自动化协议（SCAP）技术规范：SCAP V7.7，2011 年 2 月
11. NIST SP 800-128，信息系统安全配置管理指南，2011 年 8 月
12. NIST 跨部门报告（IR）7756，草拟版，CAESARS 框架扩展：企业持续监控技术参考架构，2011 年 2 月

其他

1. 通用漏洞披露（CVE），http://cve.mitre.org/about/index.html
2. 通用漏洞评分系统（CVSS），http://www.first.org/cvss/

附录 B 术语表

常用术语定义

本附录列举了 SP 800-137 文件所使用的安全术语定义。术语表中的术语与 NIST 制定的 FISMA 相关安全标准与指南系列中的定义一致。除非另有说明，本文件中所有术语还与国家安全系统委员会（CNSS）第 4009 号命令《国家信息保障术语表》中的定义一致。

活动 *[NISTIR 7298]*	评估对象，指针对某一信息系统的由人所从事的特定防护工作或行动，如进行系统备份操作、监控网络流量等。
充分安全 [OMB Circular A-130，附录 III]	可应对风险以及信息泄露、误用或非法访问或修改导致的危害，包括通过使用高成本效益的管理、人员、运营及技术控制措施来保证机构所使用的系统及应用有效运行，提供相称的机密性、完整性与可用性。
高级持续性威胁 [NIST SP 800-39]	具有高级专业知识与大量资源的攻击者利用多种攻击向量（如网络、物理与欺诈）挖掘机会达到自己的目的，一般是在组织的信息技术基础设施内建立、扩充据点以持续窃取信息并/或破坏/阻碍任务、计划或组织的关键工作，或准备在未来进行这样的活动。此外，这种威胁在相当长的一段时间内反复尝试，不断调整以适应防守方的防护措施，坚持维持一定水平的必要互动以实现目标。
机构	参见“执行机构”。
分配 [NISTIR 7298]	组织通过该流程确定安全控制措施是否针对特定系统、是否为混合类型或者是通用类型。组织通过该流程将安全控制措施分配给提供特定安全功能的各个信息系统部件（如路由器、服务器、远程传感器等）。
应用 [NISTIR 7298]	信息系统上运行的软件程序。
评估	参见“安全控制措施评估”。
评估结论 [NISTIR 7298]	指针对安全控制措施或控制加固措施进行评估以达到某个评估目的的过程中产生的评估结果；评估人在评估过程中给出的“满意”或其他评价结果。
评估方法 [NISTIR 7298]	评估人在评估过程中为获取证据所采取的方法（检视、面谈、测试）。
评估对象 [NISTIR 7298]	评估过程中评估方法针对的项目（规范、机制、活动、个人）。
评估目的 [NISTIR 7298]	对于目标的陈述，即对安全控制措施或控制加固措施进行评估所期望获得的结果。
评估规程 [NISTIR 7298]	评估*目的*集合及关联评估*方法*与评估*对象*集合。
评估人	参见“安全控制措施评估人”。
保障 [NISTIR 7298]	信息系统内预期安全控制措施有效应用的信心基础。
保障用例 [NISTIR 7298]	结构性论据及证据集合，可表明信息系统满足了某一质量属性的特定要求。
认证 [FIPS 200]	验证用户、流程或设备的身份，一般为访问信息系统资源的前提条件。

真实性 [CNSSI 4009]	具有真实性或可以被验证及信任；对于传输信息、消息或消息发起者合法性的置信度。参见“认证”。
授权（操作） [CNSSI 4009]	高级组织主管所作出的官方管理决定，授权操作信息系统，对于批准后安全控制措施的实施为组织运营（任务、职能、形象或声誉）、组织资产、个人、其他组织及国家带来的风险，明确表示接受。
授权范围 [NIST SP 800-37]	授权主管授权操作的信息系统的所有部件，不包括与该信息系统相连的单独授权的系统。
授权主管（AO） [CNSSI 4009]	在组织运营（任务、职能、形象或声誉）、组织资产、个人、其他组织及国家可接受风险范围内，对信息系统操作负责的高级（或联邦）官员或主管。
可用性 ***[44 U.S.C.，Sec. 3542]***	保证信息可及时并可靠访问及使用。
分类	参见“安全分类”。
首席信息官（CIO） ***[PL 104-106，Sec. 5125（b)]***	机构官员，其责任包括： 1) 为执行机构领导和机构的其他高级管理人员提供建议与其他帮助，保证获取信息技术，按法律、行政命令、指令、指导方案、规定及机构领导所规定优先级的要求管理信息资源； 2) 为机构开发、维护并协助实施健全的信息技术架构； 3) 促进机构的所有主要信息资源管理流程的有效设计与运行，包括优化机构的工作流程。
首席信息安全官	参见“高级机构信息安全主管”。
通用控制措施 [CNSSI 4009]	通用控制措施承继于一个或多个组织信息系统。参见“安全控制措施承继”。
通用控制措施提供人 [NISTIR 7298]	负责开发、实施、评估与监控通用控制措施（如承继于信息系统的安全控制措施）的组织内高级职员。
替代安全控制措施 ***[NISTIR 7298]***	组织采用的管理、运营及技术控制措施（如预防措施或对策），作为对 NIST SP 800-53 中所述的高、中、低基线推荐控制手段的代替，为信息系统提供同等防护。
综合测试 [NISTIR 7298]	获取评估对象内部结构与实施细节详细、明确信息的测试方法，也称为“白盒测试”。
计算机事件响应小组（CIRT） [CNSSI 4009]	通常由安全分析师组成，旨在规划、推荐与协调即时缓解活动，以控制、消除与恢复计算机安全事件造成的影响，也称为“计算机安全事件响应小组（CSIRT）或计算机事件响应中心、计算机事件响应能力或网络事件响应小组（其缩写均为 CIRC）。
机密性 ***[44 U.S.C.，Sec. 3542]***	对于信息访问及披露的授权限制，包括保护个人隐私与私有信息。
配置控制（或配置管理） ***[CNSSI 4009]***	控制硬件、固件、软件及文档的更改，以防止信息系统在系统实施前后及过程中被不当修改。
持续监控	实时了解威胁信息，为组织风险决策提供支持。 参见《信息安全持续监控、风险监控及状态监控》。
受控界面	实施安全指导方案、控制互联信息系统间信息

[CNSSI 4009]	流动的机制的边界。
对策 [CNSSI 4009]	减少信息系统脆弱性的活动、设备、规程、技术或其他措施，与安全控制措施和预防措施含义相同。
覆盖度 [NISTIR 7298]	与评估方法相关的属性，描述的是评估对象范围或广度（如评估对象的类型以及各类评估对象的数量）。覆盖度属性的值包括基本、专门和综合，表示覆盖范围从小到大。
数据外泄	通过数据窃取或泄露来暴露私有、敏感或机密信息。
深度 [NISTIR 7298]	与评估方法相关的属性，描述的是方法在应用时的严格与细致程度。深度属性的值包括基本、专门和综合，表示深度从低到高。
域 ***[CNSSI 4009]***	包括一系列系统资源与系统实体的环境或情境，这些系统实体有权访问通用安全指导方案、安全模型或安全架构所定义的资源。参见“安全域”。
运行环境 [NISTIR 7298]	信息系统处理、存储与传输信息的物理环境。
检视 ***[NISTIR 7298]***	一种评估方法，典型过程是检查、检测、评审、观察、研究或分析一个或多个评估对象，以促进理解、澄清疑问或获取证据，评估结果是判断安全控制措施动态有效性的基础。
执行机构 [41 U.S.C.，Sec. 403]	5 U.S.C.第 101 节中所规定的执行部门；5 U.S.C.第 102 节中所规定的军事部门；5 U.S.C.第 104（1)节中定义的独立机构；完全受 31 U.S.C.第 91 章约束的政府全资公司。
期望输出	实施 ISCM 策略时监控、评估得来的数据。
联邦机构	参见“执行机构”。
联邦信息系统 [40 U.S.C.，Sec. 11331]	执行机构、执行机构承包人或代表执行机构的其他组织所使用、运营的信息系统。
高影响系统 [FIPS 200]	至少有一项安全目标（机密性、完整性、可用性）被 FIPS 199 评定为具有潜在高影响的信息系统。
混合安全控制措施 [CNSSI 4009]	信息系统内实施的安全控制措施，部分为通用控制措施，部分为特定系统控制措施。 参见“通用控制措施与特定系统安全控制措施”。
安全事件 [FIPS 200]	实际或潜在影响信息系统的、系统所处理、存储或传输信息的机密性、完整性或可用性的事件，或违反或有可能将要违反安全指导方案、安全规程或可接受使用策略的事件。
个人 [NISTIR 7298]	应用规范、机制或活动的评估对象类型—人。
信息 [FIPS 199]	某种信息类型的实例。
信息负责人 [CNSSI 4009]	对于特定信息具有法定或运行权限、负责控制信息生成、收集、处理、分发或处置的相关人员。
信息资源 [44 U.S.C.，Sec. 3502]	信息与相关资源，如人员、设备、资金和信息技术。
信息安全 [44 U.S.C.，Sec. 3542]	保护信息和信息系统，使其免于非法访问、使用、泄露、中断、修改或破坏，保证其机密性、完整性与可用性。

信息安全架构师 [NISTIR 7298]	保证保护组织核心任务与业务流程的信息安全要求在企业架构内被充分、全面执行的个人、团体或组织。这里的企业架构包括参考模型、部门与解决方案架构以及支持任务与业务流程实施的相关信息系统。
信息安全持续性监控（ISCM）	实时了解信息安全、漏洞及威胁，以支持组织风险管理决策。 【注意：这里的“持续”是指定期对组织的安全风险和应对措施进行评估和分析，且该频率足以为组织进行基于风险的安全决策提供支持，可对其信息进行充分保护。】
信息安全持续性监控（ISCM）项目	为基于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。
信息安全持续性监控（ISCM）流程	该流程旨在： • 定义 ISCM 策略 • 建立 ISCM 项目 • 实施 ISCM 项目 • 分析数据并报告发现 • 对监控结果做出响应 • 评审和更新 ISCM 战略与项目
信息安全项目计划 [NISTIR 7298]	一种正式文档，概述组织范围内的信息安全项目的安全需求，介绍为满足这些安全需求而采用或拟采用的项目管理控制措施及通用控制措施。
信息安全风险 [NIST SP 800-39]	可能产生的非法访问、使用、披露、中断、修改或破坏信息与/或信息系统对于组织运营（任务、职能、形象、声誉）、组织资产、个人、其他组织及国家的风险。参见“风险”。
信息系统 [44 U.S.C.，Sec. 3502]	有序的离散信息资源，其中的信息被收集、处理、维护、使用、共享、分发或处置。
信息系统边界	参见“授权范围”。
信息系统负责人（或项目经理） [NISTIR 7298]	负责信息系统整体采购、开发、集成、修改或运维的相关人员。
信息系统安全工程师 [CNSSI 4009]	从事信息系统安全工程活动的个人。
信息系统安全工程 [CNSSI 4009]	获取、细化信息安全需求、通过有针对性的安全设计或配置将这种需求集成到信息技术部件产品与信息系统中的过程。
信息系统相关安全风险	信息或信息系统机密性、完整性或可用性被破坏造成的风险，以及这种风险对于组织（资产、任务、职能、形象或声誉）、个人、其他组织及国家造成的影响。参见“风险”。
信息系统安全主管（ISSO） [CNSSI 4009]	负责维护信息系统或项目的运行安全状况的个人。
信息技术 [40 U.S.C.，Sec. 1401]	用于执行机构自动化获取、存储、利用、管理、移动、控制、展示、交换、互通、传输或接收数据或信息的设备或互联系统或设备子系统。为达到上述目的，执行机构直接使用设备或执行机构承包人根据下述合同要求使用设备：（1）要求使用该种设备；或（2）要求提供服务或设备时重点使用该设备。“信息技术”包括计算机、辅助设备、软件、固件及其类似过程、服务（包括支持性服务）与相关资源。

信息类型 [FIPS 199]	组织或在某些情况下由特定法律、行政命令、指令、指导方案或规定所定义的分类信息（如隐私、医药、私有、金融、调查、承包人敏感或安全管理数据）。
完整性 [44 U.S.C.，Sec. 3542]	对于不当信息修改或破坏的防护，包括保证信息的抗抵赖性与真实性。
访谈 [NISTIR 7298]	一种评估方法，典型过程是与组织内的个人或团体进行沟通，以促进理解、澄清疑问或获取证据，评估结果是判断安全控制措施动态有效性的基础。
入侵检测和防御系统（IDPS） [NISTIR 7298]	该软件自动监控计算机系统或网络中事件，对事件进行分析，以发现或有安全事件迹象，并尽力阻止检测到的或有安全事件。
恶意软件 [NISTIR 7298]	恶意软件是一种程序，悄悄潜入系统，旨在损害受害者的数据、应用或操作系统的机密性、完整性和可用性，或者骚扰或干扰受害者。
管控措施 [FIPS 200]	信息系统的安全控制措施（如防护措施或对抗措施），主要关注风险管理和信息系统安全管理。
机制 [NISTIR 7298]	评估对象包括信息系统内部或边界需防护的部件（如硬件、软件或固件）。
指标 [NISTIR 7298]	这些工具通过收集与分析信息并上报相关性能数据，方便了决策，提升了性能，加强了问责。
国家安全系统 [44 U.S.C.，Sec. 3542]	机构、机构的承包商或代表机构的其他组织使用或运营的信息系统（包括任何电信系统）：（i）系统的功能、运行或使用涉及情报活动、与国家安全相关的加密活动、军队的命令与控制、以及作为武器或武器系统的不可或缺的一部分的设备，或对军事事务或情报任务的直接实现起关键作用（不包括用于日常行政和业务应用的系统，如工资发放、财务、后勤和人事管理应用）；（ii）一直通过信息保护流程保护的系统。基于国防利益或外交政策的考虑，这些流程已获得根据《行政命令》或《国会法案》制定的标准的特别授权，在执行过程中确保信息安全。
运营控制措施 [FIPS 200]	信息系统的安全控制措施（如防护措施或对抗措施）一般通过手动执行和实现（而非通过系统实现）。
组织 [FIPS 200, Adapted]	组织结构中任意规模、复杂性或位置的实体（如联邦机构或该机构酌情设立的任意运营部门）。
组织的信息安全持续性监控	根据组织的风险容忍度，在汇报结构内（旨在实现数据驱动的实时风险管理决策），对安全控制措施的实施和组织的安全状态进行评估，以确保针对系统、网络和网络空间的安全控制措施的有效性。
补丁管理 [CNSSI 4009]	对操作系统和应用软件代码的修订进行的系统性通知、识别、部署、安装和验证。这些修订包括补丁、热修复和补丁包。
渗透测试 [NISTIR 7298]	渗透测试是一种测试方法，指评估人利用现有文档（例如系统设计、源代码和手册），在特定约束条件下进行测试，试图绕过信息系统的

	安全特性。
行动计划和里程碑（POA&M） [OMB 备忘录02-01]	此文档用于识别需执行的任务。此文档中详细描述了计划中各阶段所需的资源，任务执行过程中的里程碑、以及实现这些里程碑的预期日期。
潜在影响 [FIPS 199]	数据保密性、完整性和可用性的丧失可能会对组织运营、组织的资产或个人带来：（i）有限的负面影响（FIPS 199低风险）；（ii）严重的负面影响（FIPS 199中风险）；（iii）恶劣或灾难性的负面影响（FIPS 199高风险）。
记录 [CNSSI 4009]	作为所举行活动和达成结果（如表格、报告和测试结果）的记录(自动或手动生成的)证明。这些记录可作为判断组织和信息系统是否按照预期运行的依据。同时，也可查阅各组相关数据字段，如那些可由程序访问，且包含特定条目的完整信息的数据字段组。
弹性 [NIST SP 800-39, Adapted]	弹性指以下两种能力：（i）在恶劣条件或强大压力下，甚至是恶化或糟糕的状态下，保持基本运营能力。（ii）在业务要求的时间范围内恢复到有效运营状态。
风险 [FIPS 200, Adapted]	衡量潜在情形或事件，且通常为实体本身的某一功能，为实体带来的威胁程度：（i）若情形或事件发生，所带来的负面影响。（ii）发生的可能性。 注意：信息系统相关的安全风险指由于信息或信息系统的保密性、完整性或可用性的丧失而带来的风险。这些风险反映了对组织运营（包括任务、职能、形象或声誉）、组织资产、个人、其他组织或国家带来的潜在负面影响。例如，对国家的负面影响包括对以下信息系统的损害：支持关键基础设施应用的系统或对于国土安全部规定的政府持续性运营起关键作用的系统。
风险评估 [CNSSI 4009]	风险评估指确定信息系统的运行为组织的运营（包括任务、职能、形象和声誉）、组织资产、个人、其他组织或国家带来的风险的过程。风风险评估是风险管理的一部分，包括威胁和漏洞分析，并考虑已采用或拟采用的安全控制措施带来的风险缓解。这一过程与风险分析类似。
风险主管（职能） [CNSSI 4009]	组织内的个人或团队，其职责是确保：（i）从组织为开展业务和履行业务职能而制定的整体战略目标的角度，考虑各信息系统的安全风险，包括授权决策。（ii）统一管理整个组织的信息系统相关的安全风险，且其管理反映组织的风险容忍度，并与影响组织使命/业务成功的风险一并考虑。
风险管理 [FIPS 200, Adapted]	对组织运营（包括业务、职能、形象和声誉）、组织资产、个人、其他组织和国家的信息安全风险进行管理的计划和相关流程，包括：（i）构建进行风险相关活动的环境；（ii）评估风险；（iii）确定风险后，采取响应措施；（iv）持续监控风险。
风险监控	持续关注组织的风险环境、风险管理计划以及相关活动，为风险决策提供支持。

风险响应 [NIST SP 800-39]	接受、规避、缓解、分享或转移有关组织运营（任务、职能、形象或声誉）、组织资产、个人、其他组织和国家的风险。
风险容忍度 [NISTIR 7298]	实体为实现潜在期望结果而情愿承受的风险级别。
防护措施 [CNSSI 4009]	为实现信息系统的安全需求（如保密性、完整性和可用性）而制定的保护措施。防护措施包括安全特性、管理约束、人员安全以及物理结构、地区和设备的安全。这与安全控制措施和对策类似。
安全授权	请参见“授权”。
安全自动化域	信息安全领域，包括各类工具、技术和数据。
安全分类 [CNSSI 1253, FIPS 199]	确定信息或信息系统的安全类别的过程。安全分类方法在CNSS指令1253（针对国家安全系统）以及FIPS 199标准（针对非国家安全系统）中进行了介绍。
安全控制措施评估 [CNSSI 4009, Adapted]	对信息系统的管理、运营和技术方面的安全控制措施进行测试和评估以确定这些措施实施的准确程度、其运行与期望结果之间的差异以及在满足系统安全需求方面与预期结果之间的差异。
安全控制措施评估人 [NISTIR 7298]	负责安全控制措施评估的个人、团队或组织。
安全控制措施基线 [FIPS 200, Adapted]	NIST特别刊物800-53和CNSS指令1253中为联邦信息系统定义的一组最小安全控制措施。
安全控制措施有效性	衡量安全控制措施实施的准确性（安全控制措施的实施与安全计划的匹配程度），并根据当前风险容忍度，评估安全计划对组织需求的满足程度。
安全控制措施继承 [CNSSI 4009]	指下列情况：信息系统或应用由安全控制措施（或部分安全控制措施）进行防护，且这些措施的制定、实施、评估、授权和监控由负责系统或应用以外的实体负责；系统或应用所在组织的内部或外部实体。请参见“通用控制措施”。
安全控制措施 [FIPS 199]	针对信息系统制定的有关管理、运营和技术方面的控制措施（如防护措施或对策），以保护系统及其信息的保密性、完整性和可用性。
安全域 [CNSSI 4009]	可实现安全指导方案并由单一机构管理的域。
安全影响分析 [NIST SP 800-53]	组织的工作人员为确定信息系统的变化对系统安全状态的影响程度而进行的分析。
安全事件	请参见“事件”。
安全管理仪表盘 [NIST SP 800-128]	对有关组织安全状态的准实时信息进行合并的工具，且将合并的信息展现给安全管理相关利益主体。
安全目标 [FIPS 199]	保密性、完整性或可用性。
安全计划 [NISTIR 7298]	一种正式文档，概述信息系统或信息安全计划的安全需求，介绍为满足安全需求而已采用的或拟采用的安全控制措施。请参见“系统安全计划”或“信息安全项目计划”。
安全指导方案 [CNSSI 4009]	提供安全服务的一套标准。
安全状况 [CNSSI 4009]	组织的网络、信息和系统的安全状态。这些系统基于信息架构（IA）资源（如人员、硬件、

	软件和策略）以及组织现有的防御管理能力和随机应变的能力。
安全需求 [FIPS 200]	信息系统的安全需求。这些需求源自适用的法律、行政命令、指示、策略、标准、指令、规定、规程或组织任务/业务案例需求，确保信息在处理、存储或传输过程中的保密性、完整性和可用性。
安全状态	参见安全状况。
高级（机构）信息安全主管（SISO） [44 U.S.C.，Sec. 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的授权主管、信息系统负责人和信息系统安全主管之间的主要联络人。 注意：联邦政府机构的下属组织可能使用高级信息安全主管或首席信息安全主管指代与高级机构信息安全主管的职责类似的职位。
高级信息安全官	参见“高级机构信息安全主管”。
规范 [NISTIR 7298]	评估对象，包括信息系统相关的基于文档的工件（如策略、规程、计划、系统安全需求、功能规范和架构设计）。
状态监控	对组织在信息安全持续监控战略中制定的信息安全指标进行监控。
子系统 [NISTIR 7298]	信息系统的主要分支，由信息、信息技术和执行一个或多个特定功能的人员组成。
系统	参见“信息系统”。
系统开发生命周期（SDLC） [CNSSI 4009]	系统相关活动的范围，包括系统启动、开发、收购、实现、运营和维护以及最终处置。
系统开发生命周期（SDLC） [CNSSI 4009，Adapted]	系统相关活动的范围，包括系统启动、开发、收购、实现、运营和维护以及最终处置。一个系统的处置会促使另一个系统的启动。
系统安全计划 [FIPS 200]	一种正式文档，概述信息系统的安全需求，介绍为满足安全需求而已采用的或拟采用的安全控制措施。
针对于系统的安全控制措施 [CNSSI 4009]	针对于信息系统的安全控制措施，且此措施尚未设置为通用安全控制措施或作为将在信息系统内实施的混合型监控措施的一部分。
定制 [CNSSI 4009]	基于以下方面对安全控制措施基线进行修改的流程：（i）范围确定指南的应用；（ii）补充性安全控制措施的规范（如有需求）；（iii）有关组织如何通过明确指定和选择语句，在安全控制措施中定义参数的规范。
技术控制措施 [FIPS 200]	信息系统的安全控制措施（如防护措施或对抗措施），一般由信息系统通过其硬件、软件或固件中的机制进行实施和执行。
测试 [NISTIR 7298]	一种评估方法类型，其特点如下：在特定条件下执行一种或多种评估对象，将实际行为与期望行为进行对比，其对比结果作为判断一段时间内的安全控制措施是否有效的依据。
威胁 [CNSSI 4009，Adapted]	指以下情形或事件：对信息系统的未授权访问、损害、信息披露或修改和/或拒绝服务可能会对组织运营（包括任务、职能、形象或声誉）、组织资产、个人、其他组织或国家造成潜在不利影响。
威胁信息 [CNSSI 4009，Adapted]	针对信息系统安全的对立面的趋势、技术或手段的分析洞察。

威胁源 [FIPS 200]	旨在蓄意实现漏洞利用或通过某一形势和方法意外触发漏洞的意图和手段。这与威胁因素类似。
漏洞 [CNSSI 4009]	信息系统、系统安全程序、内部控制措施或实现中存在的可由威胁源进行利用或触发的缺陷。
漏洞评估 [CNSSI 4009]	对信息系统的漏洞的正式描述和评估。
白盒测试	参见“综合测试”。

附录 C 缩略语

AO	Authorizing Official	授权主管
CAPEC	Common Attack Pattern Enumeration & Classification	通用攻击模式列表和分类
CIO	Chief Information Officer	首席信息官
CIRT	Computer Incident Response Team	计算机事件响应小组
COTS	Commercial Off-The-Shelf	商用现货
CVSS	Common Vulnerability Scoring System	通用漏洞评分系统
CVE	Common Vulnerabilities and Exposures	通用漏洞披露
CWE	Common Weakness Enumeration	通用缺陷列表
CWSS	Common Weakness Scoring System	通用缺陷评分系统
DLP	Data Loss Prevention	数据泄露防护
FDCC	Federal Desktop Core Configuration	联邦桌面核心配置
FISMA	Federal Information Security Management Act of 2002	2002联邦信息安全管理法案
IDPS	Intrusion Detection and Prevention System	入侵检测和防御系统
ISCM	Information Security Continuous Monitoring	信息安全持续性监控
ISO	Information System Owner	信息系统所有者
ISSO	Information System Security Officer	信息系统安全主管
IT	Information Technology	信息技术
NCP	National Checklist Program	国家清单计划
NVD	National Vulnerability Database	国家漏洞数据库
OCIL	Open Checklist Interactive Language	开放检查表交互式语言
OMB	Office of Management and Budget	管理和预算办公室
OVAL	Open Vulnerability and Assessment Language	开放式漏洞和评估语言
PII	Personally Identifiable Information	个人验证信息
PM	Program Management	项目群管理
POA&M	Plan Of Action & Milestones	行动与里程碑计划
RMF	Risk Management Framework	风险管理框架
SAR	Security Assessment Report	安全评估报告
SCAP	Security Content Automation Protocol	安全内容自动化协议
SDLC	System Development Life Cycle	系统开发生命周期
SIA	Security Impact Analysis	安全影响分析
SIEM	Security Information and Event Management	安全信息与事件管理
SISO	Senior Information Security Officer	高级信息安全主管
SP	Special Publication	特别刊物
SwAAP	Software Assurance Automation Protocol	软件保障自动化协议
USGCB	United States Government Configuration Baseline	美国政府配置基线
XCCDF	Extensible Configuration Checklist Description Format	可扩展配置清单描述格式
XML	Extensible Markup Language	可扩展标记语言
AO	Authorizing Official	授权主管
CAPEC	Common Attack Pattern Enumeration & Classification	通用攻击模式列表和分类

CIO	Chief Information Officer	首席信息官
CIRT	Computer Incident Response Team	计算机事件响应小组
COTS	Commercial Off-The-Shelf	商用现货
CVSS	Common Vulnerability Scoring System	通用漏洞评分系统
CVE	Common Vulnerabilities and Exposures	通用漏洞披露
CWE	Common Weakness Enumeration	通用缺陷列表
CWSS	Common Weakness Scoring System	通用缺陷评分系统
DLP	Data Loss Prevention	数据泄露防护
FDCC	Federal Desktop Core Configuration	联邦桌面核心配置
FISMA	Federal Information Security Management Act of 2002	2002联邦信息安全管理法案
IDPS	Intrusion Detection and Prevention System	入侵检测和防御系统
ISCM	Information Security Continuous Monitoring	信息安全持续性监控
ISO	Information System Owner	信息系统所有者
ISSO	Information System Security Officer	信息系统安全主管
IT	Information Technology	信息技术
NCP	National Checklist Program	国家清单计划
NVD	National Vulnerability Database	国家漏洞数据库
OCIL	Open Checklist Interactive Language	开放检查表交互式语言
OMB	Office of Management and Budget	管理和预算办公室
OVAL	Open Vulnerability and Assessment Language	开放式漏洞和评估语言
PII	Personally Identifiable Information	个人验证信息

附录 D 实现 ISCM 的技术

组织可通过采用技术使很多 ISCM 活动实现自动化，从而为组织风险管理政策和战略、运营安全、内部和外部合规、报告和文档需求提供支持。这样，组织会更有效的利用其安全预算。组织也可选择采用一个参考架构如 NIST CAESARS 框架扩展，实现 ISCM 技术[44]。并且，组织可采用各类工具和技术，高效地收集、汇总、分析和上报数据，这些数据上至持续监控企业架构和运营环境的安全状态，下及监控各信息系统部件。这些工具和技术可实现且助力自动监控，以支持组织的流程，包括但不限于：

1) 安全控制措施有效性的持续性评估
2) 向安全责任人上报合理粒度的安全状态
3) 风险管理和风险缓解活动的验证与评估
4) 内部和外部高级需求的合规保障
5) 运营环境变化的安全影响分析

本附录中涉及的工具和技术旨在实现整体 ISCM 计划的战略、指导方案、角色和职责方面的杠杆效应，并协助组织自动化实施、评估、持续监控数项 NIST SP 800-53 安全控制措施。尽管这些工具和技术主要用于对可实现自动化的技术性安全控制措施进行持续性监控，但可自动提供依据证实非技术性的安全控制措施或不能轻易实现自动化的某些安全控制措施的存在及其有效性。自动化的实现手段包括各类商用现有产品和政府现有产品、内置的操作系统能力、自定义工具以及采用标准的自动化规范的脚本。

了解并认识到需对安全控制措施的有效性进行评估是非常重要的，尤其对非技术性安全控制措施的定期评估。自动化工具所收集的数据或许并未反映出非技术性安全控制措施的存在和有效性，但某些情况下，我们可根据这些数据推断非技术性安全控制措施的有效性。尽管我们可能无法使用自动化工具和技术按照指导方案和规程进行监控，但可对相关的安全目标进行监控。

开放检查表交互式语言（见 D.3.1 节）可用于将那些需人工交互且可通过问答形式进行验证的控制措施进行半自动化。例如，可创建一份自动化调查问卷，用于收集年度安全意识培训相关的信息。

自动化工具所持续或按需收集的安全相关信息的有效性反映了基础管理与所采用的安全控制措施的有效性。既然如此，自动化工具和技术的价值，包括直接进行数据收集、汇总和分析的工具和技术，取决于支持其使用的操作流程。为使组织实现运营方面的安全效益并使工具和技术反馈准确的安全状态，相关负责人应对这些工具、技术和所有基础安全控制措施进行筛选、实施、运行和维护，解读所获取的监控数据，并选择和实施合适的修复技术。

本附录介绍了各种工具和技术在 ISCM 活动自动化过程中发挥的作用。同时，也介绍了通用工具、技术和开放性规范，它们用于收集、分析和有意义地展示数据，如信息资产洞察、威胁和漏洞感知以及安全控制措施的有效性。这些数据为组织的安全状态持续性监控提供了支持。此外，本节还介绍了可通过各种技术实现自动化安全控制措施的实例，但并非涵盖全部实例。新产品和新技术持续涌入市场。那些通常已完成自动化但未作为与以下技术相关的实例出现的控制措施包括其自动化通过操作系统内置的能力、自定义工具和脚本或几种工具和能力[45]的组合完成的控制措施。

D.1数据收集技术

数据收集技术能够针对已知安全威胁和漏洞提供观察、检测、防护或记录能力，且（或）修复或管理为解决威胁和漏洞而实施的各类安全控制措施。这些技术一般在信息系统层（3 层）上实施。我们可配置这些技术，为在任务/业务流程和信息安全治理指标的实施过程中实现组

[44]如欲了解更多信息，请参见 NISTIR 7756 修正草案，“CAESARS 框架扩展：企业持续监控技术参考架构”。

[45] 可通过安全工程或专有/第三方软件和日志管理工具，实现完全自动化或半自动化的控制措施包括账户管理、安全培训记录、安全事件上报和物理访问控制措施。

织的持续性安全监控需求而提供支持。在组织范围内执行数据收集工具可使组织系统继承和利用上述能力。

安全自动化域指涵盖工具、技术和数据的信息安全领域。可对这些域中的数据进行捕获、关联、分析和上报，以展现由所监控的域代表的组织的安全状态。安全自动化提供标准化规范，可实现不同域间的互操作性和数据流。可通过各种工具和技术实现数据监控能力。所收集信息的粒度由组织依据其监控目标和企业架构的能力确定，从而为以上活动提供支持。

本节主要介绍 11 个安全自动化域内用于支持持续性监控的工具和技术：

- 漏洞管理
- 补丁管理
- 事件管理
- 安全事件管理
- 恶意软件检测
- 资产管理
- 配置管理
- 网络管理
- 证书管理
- 信息管理
- 软件保障

图 D-1 展示了安全自动化域。

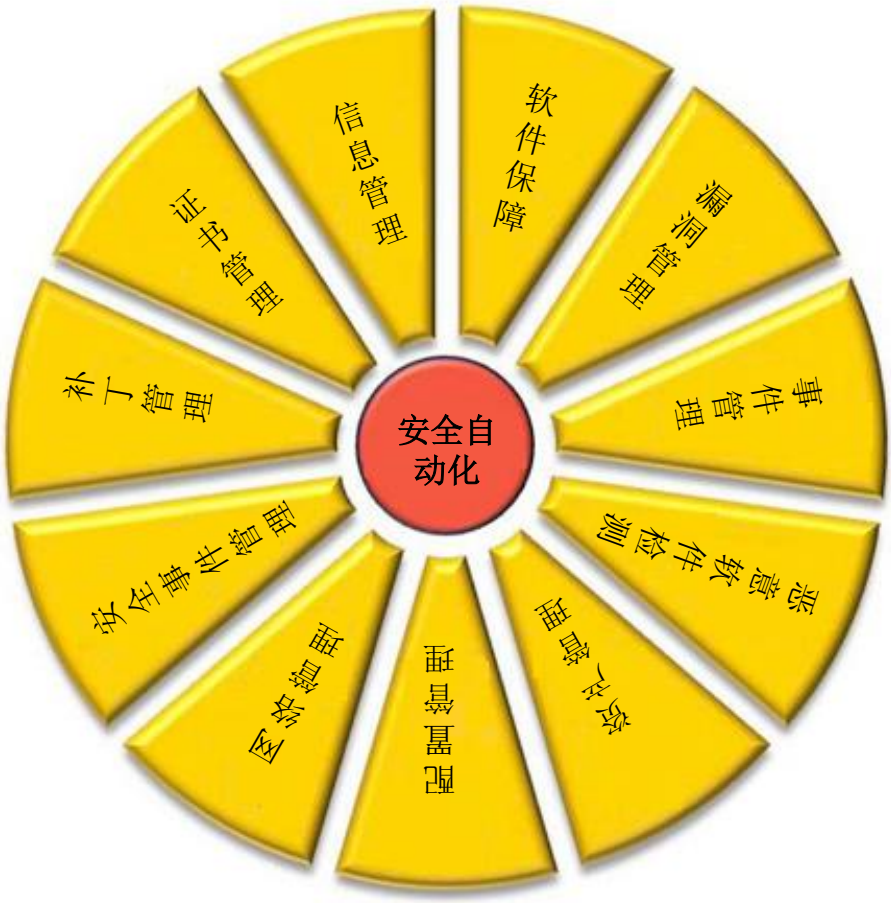


图 D-1 安全自动化域

D.1.1　漏洞管理与补丁管理

漏洞是一种软件缺陷，可导致潜在安全风险。越来越多的漏洞被发现，随之开发了更多补丁修复这些漏洞，致使人工修复系统和系统部件越来越困难。组织应尽可能利用自动化漏洞和补丁管理工具和技术在组织范围内统一识别、上报和修复漏洞。

漏洞扫描器一般用于识别组织的主机、网络以及常用操作系统和应用中的已知漏洞。这些扫描工具可主动发现漏洞、快速便捷地评估风险、识别过时的软件版本，验证是否符合组织的安全指导方案，并生成有关已识别漏洞的告警和报表。

补丁管理工具扫描组织的修复方案中涉及的系统和系统部件的漏洞，提供受影响设备所需的补丁和软件更新的相关信息，可使管理员确定补丁实施流程。各厂商提供补丁管理工具和实用程序，协助软件补丁的自动识别、发布和上报。安装补丁前必须了解补丁所产生的影响，且须按配置的补丁管理政策部署补丁，确保系统的核心功能不会因补丁的意外副作用而失效。在补丁无法部署的情况下，需采用其他安全控制措施进行补充。

漏洞评估和补丁管理技术[46]实施与有效使用可协助组织自动化实施、评估、持续监控数项 NIST SP 800-53 安全控制措施，包括 SI-2 缺陷修复、CA-2 安全评估、CA-7 持续监控、CM-3 配置变化控制、IR-4 安全事件处理、IR-5 安全事件监控、MA-2 受控维护、RA-5 漏洞扫描、SA-11 开发人员安全测试以及 SI-11 错误处理。漏洞评估和补丁管理技术可提供支持性数据，协助组织响应配置和漏洞管理方面更高的上报需求。

D.1.2　事件与安全事件管理

事件管理指对网络或系统中所观察到的事件进行监控，并在必要时进行响应。可采用各类工具和技术，如入侵检测系统和日志机制，对事件进行监控。有些工具基于已知攻击特征进行事件检测，而有些则对可能被视为攻击的行为或异常行为进行检测。某些事件可能预示着以下安全事件已经发生：包括违反计算机安全策略、可接受的使用策略或标准的计算机安全实践，或是因违反这些政策而导致迫近的威胁。安全事件管理工具可帮助检测针对组织的恶意网络攻击、对其进行响应，并限制产生的后果。

日志是对组织内的系统和网络中发生的事件的记录。日志由日志条目组成。每个日志条目包含系统或系统部件内发生的特定事件的信息。组织的很多日志均包含有关计算机安全的记录。计算机安全日志有多个来源，包括安全软件（如恶意软件防护软件）、防火墙、入侵检测和防御系统、服务器操作系统、工作站、联网设备以及各类应用。

安全日志的种类和数量均有了大幅增长，且所占的存储空间也越来越大。因此非常有必要对信息系统的安全日志进行管理，即安全日志数据的生成、传输、存储、分析和处理过程。对于确保在适当的时间内保存足够详尽的安全记录而言，日志管理是至关重要的。日志可为审计分析、取证分析、内部调查、基线设定以及运行趋势和长期问题的识别提供参考数据。常规日志分析有助于识别安全事件、策略违规事件、欺诈活动、运行问题，从而为 ISCM 能力提供支持。

日志记录与日志管理工具和技术的实施与有效使用可协助组织自动化实施、评估、持续监控数项 NIST SP 800-53 安全控制措施，包括 AU-2 可审计的事件、AU-3 审计记录内容、AU-4 审计存储能力、AU-5 针对审计处理失败的响应、AU-6 审计复核、分析和上报、AU-7 审计精选与报告生成、AU-8 时间戳、AU-12 审计生成、CA-2 安全评估、CA-7 持续监控、IR-5 安全事件监控、RA-3 风险评估以及 SI-4 信息系统监控。

入侵检测指如下过程：监控计算机系统或网络中发生的事件并进行分析以识别潜在安全事件，包括违反计算机安全策略、可接受的使用策略或标准的计算机安全实践，或是因违反这些政策而导致迫近的威胁。入侵防护指进行入侵检测并试图阻止检测到的可能发生的安全事件的过程。入侵检测和防御系统（IDPS）主要专注于识别、记录和试图阻止潜在安全事件，并上报给安全管理员进行进一步分析和处理。

通常，入侵检测和防御系统记录所检测到的事件的相关信息，将重要事件上报给安全管理员，并自动生成报表。安全管理员查看报表后，采取手动修复措施。很多入侵检测和防御系统进行配置后，可利用各种技术，如修改安全配置或阻断攻击，对所检测到的威胁做出响应。

在 ISCM 计划中，入侵检测和防御系统可用于提供数据作为判断安全控制措施（如策略、规程及实现的其他技术控制措施）是否有效的依据、记录当前威胁，并阻断针对信息系统的未授权使用。入侵检测和防御系统的实施和有效使用可协助组织自动化实施、评估、持续监控数项 NIST SP 800-53 安全控制措施，包括 AC-4 信息流实施、AC-17 远程接入、AC-18 无线接入、AU-2 可审计的事件、AU-6 审计复核、分析和上报、AU-12 审计生成、AU-13 信息披露监

[46]如欲了解更多信息，请参见 NIST SP 800-400 修订版中的“创建补丁和漏洞管理计划”。

控、CA-2 安全评估、CA-7 持续监控、IR-5 安全事件监控、RA-3 风险评估、SC-7 边界防护、SI-3 恶意代码防护、SI-4 信息系统监控以及 SI-7 软件和信息完整性。入侵检测和防御系统也可提供支持性数据助力组织满足计算机应急响应小组提出的安全事件上报要求，以及管理和预算办公室和机构提出的首席信息官有关系统和连接清单、安全事件管理、边界防护和配置管理方面的上报要求。

D.1.3　恶意软件检测

恶意软件检测能够识别并上报目标系统本身或发往此系统的病毒、木马程序、间谍软件或其他恶意代码。组织通常会在信息系统的出入口（如防火墙、邮件服务器、web 服务器、代理服务器或远程访问服务器）以及端点设备（如工作站、服务器或移动计算设备）处部署恶意软件检测机制，用于检测并清除恶意代码。这些恶意代码可能通过电子邮件、邮件附件、web 接入、可移动媒介或其他方式携带或通过利用信息系统的漏洞注入。

可配置恶意软件检测机制对信息系统进行周期扫描，并在依据组织的安全策略下载、打开或执行外部文件时，对其实时扫描。恶意软件检测机制经常会依据所设置的动作对发现的恶意代码进行相应处理。

除了恶意软件检测，还可采用各种技术和方法限制或消除恶意代码攻击的影响。若与配置管理和控制规程和强大的软件完整性管理措施配合使用，恶意软件检测机制会更有效地阻止未授权代码的执行。其他风险缓解措施包括安全编码实践、可靠的采购流程、对安全配置定期监控，有助于防止使用未授权的功能。

恶意软件检测技术的实施与有效利用可协助组织自动化实施、评估、持续监控数项 NIST SP 800-53 安全控制措施，包括 CA-2 安全评估、CA-7 持续监控、IR-5 安全事件监控、RA-3 风险评估、SA-12 供应链保护、SA-13 信誉、SI-3 恶意代码防护、SI-4 信息系统监控、SI-7 软件和信息完整性以及 SI-8 垃圾邮件防护。恶意软件检测技术也可提供支持性数据，助力组织满足计算机应急响应小组提出的安全事件上报要求，以及管理和预算办公室和机构提出的首席信息官有关安全事件管理、远程接入、和边界防护方面的上报要求。

D.1.4　资产管理

资产管理工具可协助维护组织的软件和硬件清单。为此，需结合使用系统配置、网络管理和证书管理工具，或采用专用工具。资产管理软件可跟踪组织资产的生命周期，并提供相关工具如远程资产管理和各种自动化管理功能。

资产管理技术的实施与有效使用可协助组织自动化实施、评估、持续监控数项 NIST SP 800-53 安全控制措施，包括 CA-7 持续监控、CM-2 基线配置、CM-3 配置变化管理、CM-4 安全影响分析、CM-8 信息系统部件清单以及 SA-10 开发人员配置管理。

D.1.5　配置管理

管理员可利用配置管理工具配置相关设置、监控配置变化、收集配置状态，并在必要时恢复配置。要管理信息系统和网络部件的众多配置，几乎无法通过手动完成。而采用自动化方案可降低配置管理成本，提升效率，增强可靠性。

系统配置扫描工具可自动审计和评估目标系统，以确定是否符合已设定的安全基线配置。用户可确定是否符合安全基线配置、明确与基线配置之间的差距，并制作有关操作系统和/或应用的检查单。

如果信息系统或系统部件的配置与组织的基线配置和《系统安全计划》中的经核准的安全配置不同步，组织人员及系统负责人可能会产生错误的安全感。这就导致在某些情况下，他们明明可采取相应措施减少漏洞并保护组织免受攻击，却错失了良机。通过监控活动，组织可更好地把握安全指标要求进行监控的信息系统的安全状态。

利用身份和账户配置管理工具，组织可管理身份凭证、访问控制、授权及其权限。并且，身份管理系统可基于身份凭证实现物理访问控制并对其进行监控。身份和账户配置管理工具通常可自动化执行各种任务，如账户密码重设和其他账户维护活动。这些系统可监控并上报各种活动，如登录失败、账户锁定和资源访问。

组织可采用各种配置管理工具为其需求提供支撑。在选择工具时，组织应考虑采用那些能从各种数据源和部件提取信息的工具。此外，组织所选的工具还应符合开放性的规范，如 SCAP，

支持组织范围内的互操作性、评估和上报，可按需定制输出、并支持将数据整合至 SIEM 工具和管理仪表盘。

配置管理技术的实施与有效使用可协助组织自动化实施、评估和持续监控数项 NIST SP 800-53 安全控制措施，包括 AC-2 账户管理、AC-3 接入执行、AC-5 职责分离、AC-7 登录失败、AC-9 先前登录（接入）通知、AC-10 并发会话控制、AC-11 会话锁定、AC-19 移动设备访问控制、AC-20 外部信息系统的使用、AC-22 公共可访问内容、CA-2 安全评估、CA-7 持续监控、CM-2 基线配置、CM-3 配置变化管理、CM-5 对变化的访问限制、CM-6 配置设置、CM-7 最少功能、IA-2 识别与认证、IA-4 标识管理、IA-5 认证方管理、IA-8 识别与认证（非组织用户）、IR-5 安全事件监控、MA-5 维护人员、PE-3 物理访问控制、RA-3 风险管理、SA-7 用户安装的软件、SA-10 开发人员配置管理以及 SI-2 缺陷修复。组织范围的安全配置管理与工程技术也提供了支持性数据，协助组织满足配置和资产管理方面更高的合规报告要求。

D.1.6　网络管理

网络配置管理工具提供主机发现、清单、变化管理、行为监控以及其他网络设备管理能力。有些网络配置管理工具实现了设备管理自动化并确认设备是否符合预配置策略。网络管理工具可发现网络中未经授权的硬件和软件，如欺诈性无线接入点。

网络管理技术的实施与有效使用可协助组织自动化实施、评估和持续监控数项 NIST SP 800-53 安全控制措施，包括 AC-4 信息流实施、AC-17 远程接入、AC-18 无线接入、CA-7 持续性监控、CM-2 基线配置、CM-3 配置变化管理、CM-4 安全影响分析、CM-6 配置设置、CM-8 信息系统部件清单、SC-2 应用程序分区、SC-5 拒绝服务防护、SC-7 边界防护、SC-10 网络连接断开、SC-32 信息系统分区以及 SI-4 信息系统监控。

D.1.7　许可证管理

与系统和网络设备类似，软件与应用也可以为 ISCM 提供相关数据。使用软件资产管理工具对软件资产与许可信息进行集中管理，可跟踪许可证的合规性，监控使用状态，管理软件资产生命周期。许可证管理工具提供各种特性，可自动化管理清单、占用率监控与限制、部署以及软件和应用的补丁。

许可证管理技术的实施与有效使用可帮助组织自动化实施、评估、持续监控数项 NIST SP 800-53 安全控制措施，包括 CA-7 持续性监控、CM-8 信息系统部件清单以及 SA-6 软件使用限制。

D.1.8　信息管理

一个组织会有各种系统、网络设备、数据库及其他资产，其中储存着大量的数字信息。管理信息的位置与传输对于保护数据的机密性、完整性与可用性十分必要。

数据外泄指通过数据窃取或泄露来暴露私有、敏感或机密信息。数据窃取是有意为之，间谍活动或员工不满会造成这种情况。数据泄露是无意为之，丢失笔记本电脑、员工使用互联网存储应用储存文件或员工用 U 盘保存文件带回家中会造成这种情况。

有效的数据泄露防护（DLP）策略包括清点及分类数据、采集数据指标、制定数据新建、使用、存储、传输与处置指导方案、使用工具监控静态、在用及传输数据。DLP 工具种类多样。典型的网络与安全工具如网络分析软件、应用防火墙及入侵检测/防护系统等可用于监控数据及传输内容；专用 DLP 软件可提供诸如端口/端点控制、磁盘与文件加密以及数据库事务监控等特性。这些工具可安装在桌面、笔记本或服务器上，监控网络流量或执行软件代理功能。DLP 工具内置检测、缓解策略，如邮件告警、日志记录、拦截等。

DLP 技术的实施与有效使用可帮助组织自动化实施、评估及持续监控数项 NIST SP 800-53 安全控制措施，包括 AC-4 信息流加固、AC-17 远程访问、CA-3 信息系统连接、CA-7 持续性监控、CM-7 最低功能、SC-9 传输机密性以及 SI-12 信息输出处理与保留。

D.1.9　软件保障

NIST 软件保障指标与工具评估（SAMATE)项目将软件保障定义为“确保软件程序与产品符合 NASA《软件保障指南与标准》要求、基准与规程的有计划、有系统的活动，以助力实现：

- 可靠性：没有可利用的恶意或疏忽漏洞；
- 性能可预测：有理由相信软件可正常运行。”

现有自动化规范可用以持续监控软件保障，《软件保障自动化协议》（SwAAP)也具有此功能，现正处于开发阶段，旨在测评、枚举软件缺陷与保障案例。SwAAP 使用多种自动化规范，如列举可利用漏洞（如 CVE 漏洞）的通用缺陷列表（CWE）以及评估缺陷风险值的通用缺陷评分系统（CWSS）。SwAAP 还使用通用攻击模式列表和分类（CAPEC），这是一个对外开放的攻击模式列表，具有详尽的图式与分类，描述了利用软件的常用方法；另外还使用了恶意软件属性枚举与特征（MAEC），这个规范为加密以及基于属性（如行为、工具与攻击模式）描述恶意软件信息提供了标准化语言。

有许多软件保障工具与技术融入了这样的自动化规范，为整个软件开发生命周期提供了软件安全保证。软件保障技术的实施与有效使用可帮助组织自动化实施、评估与持续监控数项 NIST SP 800-53 安全控制措施，包括 CA-7 持续性监控、SA-4 采购、SA-8 安全工程原则、SA-11 开发者安全测试、SA-12 供应链保护、SA-13 可靠性、SA-14 关键信息系统部件以及 SI-13 可预测故障防护。

D.2汇总分析技术

汇总分析技术用于从一个或多个安全控制措施或其他直接数据收集技术采集原始数据，对这些数据进行关联、分析、描述，评估安全控制实施在全组织或局部范围内的有效性，与单纯使用一种技术相比，这种方法获得的数据更有参考意义。

本节介绍了常见的汇总分析技术类型及其对于 ISCM 能力的支持作用。安全信息与事件管理（SIEM）及管理仪表盘都是常见的汇总分析技术。

D.2.1 安全信息与事件管理（SIEM）

为了提高识别不当或异常行为的能力，组织会通过 SIEM 工具综合分析漏洞扫描信息、性能数据、网络监控及信息审计记录（日志）信息。SIEM 工具是一种集中日志记录软件，方便从多个信息系统部件收集、汇总日志以及关联分析审计记录。将审计记录信息同漏洞扫描信息关联意义重大，可基于此确定漏洞扫描的准确性，将攻击检测事件与扫描结果进行关联。

SIEM 产品通常可支持多种审计记录源，如操作系统、应用服务器（Web 服务器、邮件服务器等）及安全软件，甚至还会支持如标记阅读器之类的物理安全控制设备。SIEM 服务器分析各个审计记录源的数据，将事件同审计记录条目关联，识别重要事件并确定其优先级，经过配置，还可以发起对事件的响应。

对于所支持的每种审计记录源，一般可配置 SIEM 产品对最重要的审计记录字段进行分类（如应用 XYZ 的日志中第 12 个字段的值表示源 IP），以显著提升审计记录数据的标准化及分析、关联能力。SIEM 软件可忽略对信息系统安全不重要的数据字段，减少事件上报，最终降低 SIEM 对网络带宽与数据存储空间的占用。

SIEM 技术的实施与有效使用可帮助组织自动化实施、评估、持续监控 7 项 NIST SP 800-53 安全控制措施，包括 AC-5 任务分工、AU-2 可审计事件、AU-6 审计复核、分析与汇报、AU-7 审计缩减与报表生成、CA-2 安全评估、CA-7 持续性监控、IR-5 安全事件监控、PE-6 监控物理访问、RA-3 风险评估、RA-5 漏洞扫描以及 SI-4 信息系统监控。

D.2.2 管理仪表盘

安全管理仪表盘（或安全信息管理控制台）几乎实时地将组织安全状况信息汇总、呈现给安全管理负责人。信息安全负责人可以是技术系统管理员、高级信息安全主管（SISO）或风险主管（职能）。安全管理仪表盘直观展示信息，便于理解，可根据要求定制，为组织内担任不同工作的具体角色提供合适的信息。

最大化管理仪表盘的效益，重要的是获取上级领导的认可与支持，定义适合组织的、基于信息安全指导方案与规程的、有用的量化性能指标，并确保可获得有用的性能数据。

管理仪表盘的实施与有效使用可帮助组织自动化实施、评估与持续监控数项 NIST SP 800-53 安全控制措施，包括 AC-5 任务分工、CA-6 安全授权、CA-7 持续性监控、PM-6 信息安全性能测评、PM-9 风险管理策略、RA-3 风险评估与 SI-4 信息系统监控。

D.3 自动化与参考数据源

在全组织内管理系统安全绝非易事，原因如下：多数组织有许多系统需要加载补丁，进行安全配置，每个系统都有无数软件（操作系统和应用）需要保护。组织需要对每个系统的安全配置进行持续监控，随时了解系统与组织的安全状况。组织还需要证明其符合法规与政策的安全要求。所有这些任务若没有实现标准化与自动化都极其耗时，难免出错。另一个问题是安全工具缺乏互通。例如，用组织内部名称指代漏洞或平台导致不同工具产生的报表内容不一致，耽误安全评估、决策与漏洞修复。组织应使用标准化、自动化的方法来克服这些问题。

自动化使 ISCM 不受域范围的限制，有效捕捉、关联、分析与上报组织的整体安全状况。自动化规范与标准格式使不同域间的互操作性与数据流动成为可能。每个安全工具提供某种自动化功能，包括导入、导出数据，执行其他预先配置的、独立的操作。有些自动化功能依赖于私有方法与协议，有些使用的是标准化规范与方法。使用工具自动配置设备或修改设置时，新配置首先在测试环境中进行测试。安全自动化活动包括：

- 扫描漏洞，自动应用合适的补丁；
- 基于安全设置清单自动启用安全配置；
- 根据安全设置预配置清单进行合规扫描；
- 利用工具收集安全指标，用标准化格式将指标上报给管理控制台。

可自动化的安全活动还有很多。本文讨论的工具与技术利用多种支持协议、规范与资源，提供标准化与互通性，以实施 ISCM。

自动化规范活动指组织对格式及命名进行标准化，以描述安全与 IT 相关信息。这些数据交换标准为标准化不同厂商的工具集以及跨域互通提供了基础。最成熟、使用最广泛的是安全内容自动化协议（SCAP），这个协议用于标准化对于软件缺陷及安全配置的描述。本节介绍如何使用 SCAP、国家漏洞库（NVD）及安全配置清单以标准化格式来表示、描述数据，以支持 ISCM 项目所需的安全自动化能力及角色。

D.3.1 安全内容自动化协议（SCAP）

SCAP 系列规范[47]提供了标准化格式与命名，安全软件产品据此描述安全缺陷与安全配置信息。SCAP 作为多功能协议，支持自动化漏洞与补丁检测、安全控制合规性活动与安全评测。编制 SCAP 的目的是标准化系统安全管理、提升安全产品的互通性、促进安全内容的标准化表达。SCAP 可用于维护组织系统安全，如自动验证补丁安全、检查系统安全配置的设置、探查系统的被入侵迹象。

哪些活动可进行 SCAP 自动化

有许多现成工具可用于基于 SCAP 的自动化 ISCM 活动。SCAP 产品验证程序[48]用于测试产品是否可使用 SCAP 协议及其标准的特性与功能。

SCAP 验证程序验证如下两种漏洞与补丁扫描器：认证与未认证扫描器。认证漏洞与补丁扫描器提供如下能力：利用目标系统登录权限扫描目标系统，定位、识别已知漏洞，评估软件补丁状态以基于组织定义的补丁策略确定系统的实时安全状况。未认证漏洞扫描器提供如下能力：无需进行登录认证，通过网络评估目标系统，确定是否存在已知漏洞。启用 SCAP 的漏洞扫描器经过配置，可定期扫描互联系统，提供量化的、可复用的评测，为各系统的软件缺陷

[47] 详细信息，参见 NIST DRAFT SP800-126（修订版）《安全内容自动化协议（SCAP）1.1 版本技术规范》
[48] 欲了解更多 SCAP 验证程序信息，请登录 http://scap.nist.gov/validation/。

进行评分。此类漏洞扫描器提供全面的修复能力，并可实现互通，报表工具亦可因此提供一致的缺陷检测与汇报方法。

加载补丁、漏洞监控与修复通常是首要任务，同时还要通过集成补丁流程（经过测试）保证系统软件漏洞缓解措施的一致性。使用安全自动化技术的成熟的补丁与漏洞管理程序使组织在安全管理中变被动为主动，将系统安全维持在合理水平。

漏洞评估与补丁管理技术主要用于测试常用操作系统与应用中是否存在已知漏洞。对于定制软件与应用，在检测商用现成品（COTS）中未知、未上报或疏忽造成的漏洞时，漏洞评估与分析或会要求使用额外的、更专业的技术和方法，如 Web 应用扫描器、源代码审查、源代码分析器。这些工具也可与安全控制评估方法（如红队演练（red team exercise）与渗透测试）结合使用，进行漏洞识别。

SCAP 验证程序评估配置扫描器的性能，这些扫描器可审计、评估目标系统，以确定系统是否符合定义的安全基线配置。安全基线配置包括联邦桌面核心配置（FDCC[49]）以及根据美国政府配置基线（USGCB[50]）计划创建的配置文件（profile）。

如何实现 SCAP 协议

要在 ISCM 中实现 SCAP 协议，须使用经 SCAP 验证的工具[51]和 SCAP 核查清单自动化安全配置管理，并为多种 NIST SP 800-53 安全控制措施提供评估依据。可自定义 SCAP 核查清单，以满足组织的具体要求。SCAP 核查清单还可将系统安全配置与相应的安全要求对应起来。例如，Windows XP 安全基线配置和 NIST SP 800-53 的安全控制措施相对应。这些对应关系可表明设置是符合要求的，并能提供足够的安全。这些对应关系嵌在 SCAP 核查清单中，允许 SCAP 验证工具自动生成评估和合规依据。这可以大幅减少工作投入和降低配置管理成本。如果组织目前没有或未部署经 SCAP 验证的工具，应考虑执行 SCAP 核查清单进行安全基线配置，以便在 SCAP 验证工具可用和/或部署后，立刻投入使用。

要实现对已知软件漏洞的持续监控，SCAP 核查清单和 SCAP 验证工具可用于评估已安装的评估软件资产，并根据风险严重性衍生出缓解策略。通过使用最新的 SCAP 安全相关信息对企业架构进行定期扫描，针对配置设置和已知软件漏洞缓解，安全主管和/或系统管理员可按需了解安全网络安全的态势感知。

部分自动化控制

某些安全控制措施的实施、评估与监控可能无法通过现有的工具实现完全自动化，但它们也许能通过使用开放检查单交互语言（OCIL）实现部分自动化。OCIL 定义了一个框架，该框架包括呈现给用户的一系列问题以及应对这些问题的相应步骤。当低级检查语言（如开放漏洞与评估语言（OVAL））无法自动化某项检查时，可同时使用 OCIL 和其他 SCAP 规范（如可扩展配置检查表描述格式，XCCDF），来完成。OCIL 提供了描述和评估手动安全检查的标准方法。例如，系统用户可能要求回答：“你有保存文档的安全之所吗？”OCIL 规范能够定义问题，提供多个答案共用户选择，并根据用户的答案采取相应措施，并一一列举结果集。OCIL 的一个好处是，答案可以以标准格式返回，从而使统计分析和其他计算能够自动进行。

D.3.2 参考数据源

NIST 提供两个数据库，即 NVD 和安全配置清单，支持自动和手动的 ISCM 工作。

国家漏洞库（NVD）

NVD 是美国政府基于标准的漏洞管理数据库，使用的是 SCAP 规范。该数据可实现漏洞管理、安全测量和合规性的自动化。NVD 包括安全检查清单、安全相关的软件缺陷、错误配置、产品名称和影响范围。

NVD 里的内容是动态的。例如，漏洞随着新信息（如补丁内容）的出现而更新，检查

[49] 欲了解更多 FDCC 信息，请登录 http://fdcc.nist.gov。
[50] 欲了解更多 USGCB 信息，请登录 http://usgcb.nist.gov。
[51] 关于 SCAP 验证产品的更多信息，参见 http://nvd.nist.gov/scapproducts.cfm。

清单不断更新或加入。根据 NVD 中的可用信息，重新扫描系统，以重新评估风险和缓解新的漏洞威胁。为了实现数据的标准分布，XML 数据格式的漏洞内容每两小时更新一次。通过配置系统定时扫描和评估可能发生的变化及变化带来的相关安全风险，组织可利用标准数据实现 ISCM 自动化。

安全配置清单

2002 年的《网络安全研究与开发法案》[52]要求 NIST“制定和按需修订配置和选项清单，使每个可能在联邦政府内广泛使用的计算机硬件或软件系统相关的风险降至最低。”国家核查项目清单计划（NCP）[53]是美国政府对外开放的安全检查清单知识库。在信息安全项目中使用这些检查清单可显著降低组织的漏洞风险。

安全配置清单，有时也被称为锁定指导、固化指导或基准配置。它本质上是一个包含 IT 产品的配置说明或步骤的文档，符合安全基线。不仅 IT 厂商可以制定检查清单，企业集团、学术机构、行业机构、联邦机构和其他政府组织，以及公共和私营部门的人员都可以制定。

NCP 提供的检查清单可以用通俗的语言，也可以是 SCAP 格式。通过 SCAP 格式的检查清单，SCAP 验证工具可自动处理清单和扫描系统。检查清单子集，还提供嵌入式通用配置枚举（CCE）,与 NIST SP 800-53 安全控制措施相对应。这些安全控制措施允许将检查结果按照 NIST SP 800-53 的控制要求返回。检查清单包括以下任一内容：

- 自动设置各种安全配置的配置文件（例如：可执行文档、修改设置的安全模板、脚本）；
- 指导清单用户手动配置软件的文档（例如：文本文档）；
- 提供安全安装和配置设备推荐方法的文档；和
- 为审计、认证安全（如密码）和边界安全等活动提供指导的策略文档。

安全配置清单中的说明并非都是针对安全设置的。检查清单还包括 IT 产品的管理实践和产品安全的改善。系统攻击成功的直接原因通常都是管理不善，比如未修改默认密码或未成功应用新补丁。

检查清单比对可用于对已部署系统的安全进行审计和持续监控，以确保对基线配置的维护。通常计算机配置并不是一劳永逸的。应维护配置，因为配置可能会因为软件的安装、更新和打补丁或因为计算机与域的连接和断开而有所改变。用户也可能改变安全设置，比如用户可能觉得锁屏保护程序不方便，就会关闭该项功能。

D.4 参考模型

组织可以综合使用附录 D 中的技术、规范和参考数据源进行 ISCM 技术实现，最大化利用安全信息，提高 ISCM 规划和实施的一致性。在可能的情况下，该 ISCM 技术实施可实现数据采集、汇总和分析、报告与呈现的自动化，支持组织定义的指标。

然而，组织在整合这些技术进行 ISCM 方面面临重大挑战。通常，组织使用的是多个厂商提供的不同安全产品。因此，有必要从这些工具中提取安全相关的信息（理想情况下，这些信息是原始系统状态数据）并归一化数据，使其具有可比性（在 3 层和 1、2 层）。3 层应有能力查询和上报从多个工具中收集的数据，这些数据涵盖多个 ISCM 安全自动化域。由于很多本地的 3 层数据库涵盖了一个大企业的不同部分，3 层 ISCM 数据库定期向 2 层数据库上报数据，形成分层体系结构。依次，2 层数据库向 1 层数据库上报数据，1 层数据库可能又向更高级别的用户上报数据。在 ISCM 层级间自下而上传递数据时，数据经过提炼，因为各层复制下一层级的所有安全相关信息通常既不可能，也不明智。上层用户可查询下层数据。其中一项挑战是需要一个技术机制，允许上层查询传递到下层 ISCM 实例中。另一项挑战是，进行查询时下层 ISCM 实例可能需要分析原始数据，并产生结果。这些结果可能是调查结果（原始数据与策略的对比）或分值（调查结果的数值评估），因此查询中需要一个能够

[52] 关于《2002 年网络安全研究与开发法案》，参见 http://csrc.nist.gov/drivers/documents/HR3394-final.pdf。
[53] 关于 NCP 的更多信息，参见 http://web.nvd.nist.gov/view/ncp/repository

传达所需分析的机制。理想情况下，如果请求的数据不在 3 层，3 层 ISCM 实例则运用各种安全工具收集请求的数据。

这些挑战可以通过使用一个参考模型，迎刃而解。参考模型描述了所需工具的类型、相互关系及实现 ISCM 功能所需的角色。该模型利用或提供接口规范，将工具集成起来，以实现 ISCM 技术。模型还能为每个工具类型提供规范，使工具能够在执行组织范围内的 ISCM 时候恰当发挥自己的角色作用。

能够实现可靠集成的 ISCM 参考模型的其中一个例子就是 CAESARS 框架扩展。参见 NIST 跨部门报告（NISTIR）7756 的《CAESARS 框架扩展：企业持续监控技术参考模型（草案）》。NISTIR 7756 为持续监控参考模型提供基础。利用该参考模型，组织可将各安全工具收集的数据进行汇总、分析，并基于此类数据进行评分，提供用户查询，并展示整体态势。

该模型基于概要工作流程，描述了在 ISCM 技术实现中必要的数据移动。这些工作流程是通过模型的子系统规范（如对工具类型的要求）和工具通信的接口规范实现的。利用模型的能力取决于可用的基础设施和组织测量计划[54]的成熟度。用以支撑 ISCM 的架构须实现数据采集数据采集、存储、查询、分析、检索、上报及展示功能。

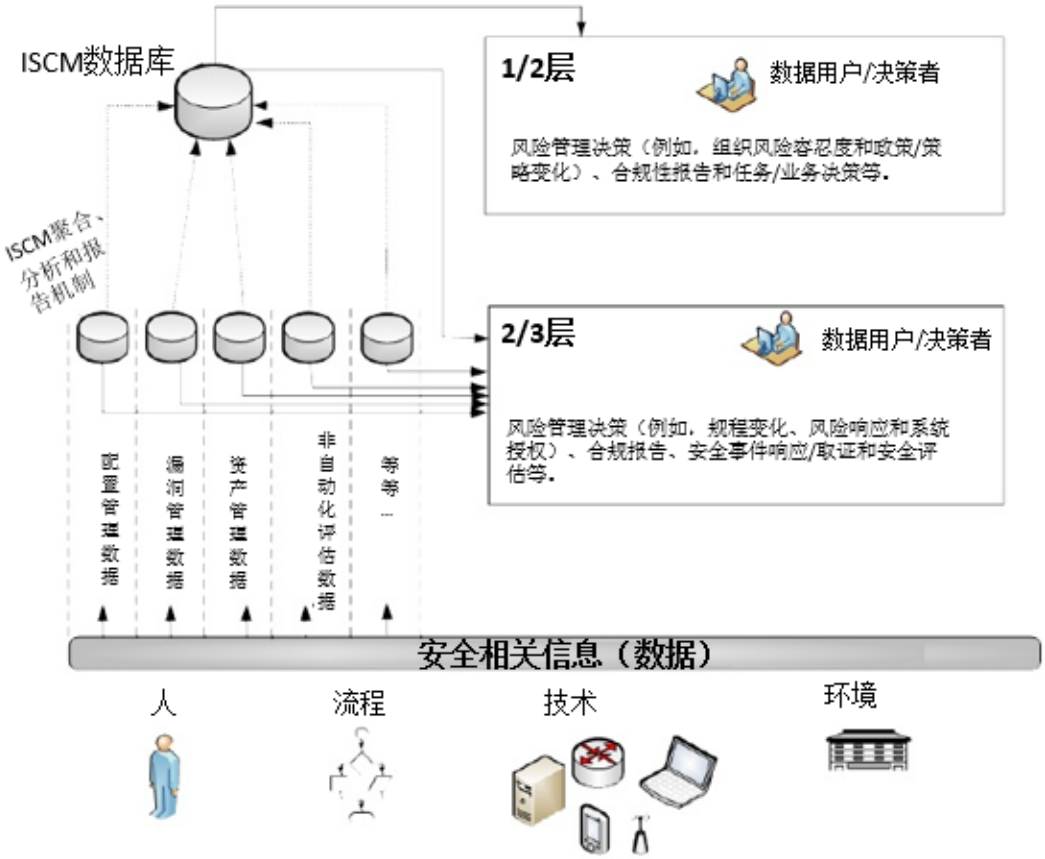
在该模型中，数据收集（用于预定义指标或对用户查询的响应）包括收集那些与安全控制实施和有效性相关的数据。数据源类型包括人、流程、技术和计算环境（包括安全控制评估结果）。可通过自动和手动方式收集数据。组织可考虑在工具内利用基于标准的方法进行数据收集，以降低集成成本，实现各种工具和技术的互通，并使数据在一次收集后可多次重复使用。人为生成的数据可通过采用自动化和标准化方法的机制进行收集。在可能的情况下，收集方法可实现标准化和自动化，实现层内和层间的信息交换、关联和分析。

收集的数据在储存时用元数据标记，以尽量复用。数据的归一化是为了汇总、关联、统一数据，以供指标使用。对于归一化或用相关属性处理的数据，在存储时应小心谨慎，避免因为清理某个指标的算法而污染另一个指标。

借助该模型，具有检索、分析和显示功能的 ISCM 基础设施能够支持在各层进行风险上报并做出基于风险的决策。可按照 ISCM 策略和既定项目来计算指标。所有安全相关信息呈现给肩负 ISCM 角色和职责的人员和其他利益相关主体，包括监控信息用户。这些用户（例如，负责补丁管理、安全控制评估和安全感知与培训的人员）使用安全相关信息并按照 ISCM 策略将操作控制在组织可容忍范围内。数据展示很灵活，能够满足各层的不同数据显示需求。

图 D-2 为 ISCM 实现流程示例，描述了在各层的安全相关信息从源数据采集、汇总与分析，到数据报告给用户的过程。用户在各层的 ISCM 数据需求各不相同。例如，3 层的系统管理员可能对支持系统层活动（比如配置变更）的技术细节感兴趣，而 1 层的管理人员可能对有利于做出组织决策（比如，安全策略的变更、安全感知项目资源的增加或安全架构的修改）的数据汇总更感兴趣。ISCM 能力的精心设计为按用户要求的格式及数据采集频率提供数据内容，协助用户做出有效决策。关于 ISCM 参考模型的更多详细信息，参见《NIST 跨部门报告 7756》。

[54] 关于测量计划的更多信息，参见 NIST SP 800-55。



图D-2 ISCM实现示例

提升关键基础设施网络安全框架

安全加社区

公益翻译项目

2016

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。