ITIL 4 信息安全管理

申明：

本系列ITIL 4实践中文版本由长河领导的ITIL先锋论坛专家委员会组织翻译，
国内众多从事ITIL理论推广及落地实践的专家们参与，需要下载最新翻译版本请关注微信

本文档翻译工作参与人员：
翻译：隗玉凯
审校：史坦晶

总审： 长河
审核： 魏钧军
统筹： 常宏

目 录

1 关于本文件

本文档提供了信息安全管理的实践指南，它分为五个主要部分，内容包括：

- 有关实践的概述
- 实践的流程和活动以及它们在服务价值链中的作用
- 实践中涉及的组织和人员
- 支持实践的信息和技术
- 实践中关于合作伙伴和供应商的注意事项。

1.1ITIL®4认证方案

本文档的选定内容可作为以下课程的一部分进行测试：

- **ITIL专家（高速IT）**

有关详细信息，请参阅相应的教学大纲文档。

2 概述

2.1 目的和描述

关键信息

信息安全管理实践的目的是对组织所需要的开展业务的信息进行保护。这包括理解和管理与信息的保密性、完整性和可用性相关的风险，以及信息安全的其他方面，例如身份验证和不可抵赖。

信息安全成为一项越来越重要又困难的任务。信息安全管理实践在数字化转型的背景下越来越重要。这是由于跨行业数字化服务的增长，在这种情况下安全信息泄露可能会对组织的业务产生重大影响。云解决方案的更广泛使用，以及合作伙伴和服务消费者的数字化服务更广泛集成产生了新的关键依赖关系，而控制信息如何被收集，存储，共享和使用的能力却有限。合作伙伴和服务使用者的处境相同，通常会在数据保护和信息安全解决方案上进行投入。但是，组织之间完整性和一致性的缺失产生了新的漏洞，需要了解和处理。信息安全管理实践与其他实践（包括：可用性管理，容量和性能管理，信息安全管理，风险管理，服务设计，关系管理，架构管理，供应商管理和其他规范）结合在一起，可确保组织的产品和服务满足所有相关方要求的信息安全级别。

许多组织认为信息安全管理实践是广义安全管理的特定分支。在服务经济中，每个组织的业务都是由服务驱动和数字化赋能的。这会带来策略更紧密的整合，因为，安全管理更关注数字化服务和信息的安全。在数字化转型消除了IT管理和业务管理边界的情形下，这种整合变为可能并发挥作用。（有关此主题的更多信息，请参见ITIL®4：高速IT）。

2.2 术语和概念

2.2.1 安全特性

信息安全管理实践有助于确保开展业务所需信息的保密性，完整性和可用性，同时需要一些活动和控制来保持这些特性。此外，信息安全管理实践通常涉及身份验证和不可抵赖。

定义：保密性

防止信息泄露给未授权实体或对未授权实体可用。

保密性是许多人在考虑信息安全时想到的第一件事。个人和组织希望确保秘密保持隐密，并且其个人信息或业务信息不被滥用。

定义：可用性

确保信息可以在需要时被使用的特性。

如果该信息在需要的时间和地点不可用，则组织无法开展其业务。

可用性管理实践考虑了服务可用性的许多方面。然而，信息安全管理实践更关注信息的可用性。

定义：完整性

确保信息准确无误，并且只能由被授权人员和活动进行修改。

不正确的信息可能比根本没有任何信息更糟糕。例如，如果一家银行错误地认为客户的帐户中有大量资金并允许他们提取该笔款项，则该银行可能遭受重大损失。

身份验证用于建立人与物的身份

定义：身份验证

验证看起来或声称是真实的特性或属性确实是真实的。

用户名和密码通常用于对人员进行身份验证，尽管通常优先推荐使用生物特征识别和安全令牌这些更严格的身份验证方式。

- 网站可以使用证书和加密来提供身份验证

定义：不可抵赖

提供不可否认的证据，证明非法事态发生，或者非法行为正在进行，并且此事态或行为由特定实体执行。

在IT系统和服务存在之前，就已经在商业交易中使用了不可抵赖技术。传统上使用签名，如果需要更高级别的证明，则可能需要对该签名进行公证。信息安全依赖不可抵赖性，因此交易可以进行。这对于保护信息完整性是必不可少的。

2.2.2 资产，威胁，威胁制造者和漏洞

定义：资产

资产是对组织具有价值的任何事物。

资产可能包括硬件，软件，网络，信息，人员，业务流程，服务，组织，建筑物或其他对组织有价值的东西。信息安全管理实践帮助组织保护资产，以便其开展业务。

2.2.3 风险管理术语

信息安全管理实践使用了许多风险管理的术语和概念。这些术语在风险管理实践中也进行了描述。

风险管理术语和定义见表2.1。

表2.1 风险管理术语

风险管理术语	定义
风险	可能造成伤害或损失，或使目标更难以实现的事态。它也可以定义为结果的不确定性，并且可以用于测量正面结果和负面结果概率的情形
控制	管理风险，确保实现业务目标或遵循流程的方法
风险处置	处理风险采取的措施。风险处置的类型包括： 风险规避：通过不执行有风险的活动来预防风险 风险调整：实施控制以降低风险的可能性或影响 风险分担：通过将一些风险传递给第三方来减少影响 风险残留：有意决定接受风险，因为它低于可接受的阈值（并且在组织的风险承受范围之内）
残余风险	应用控制之后剩余的风险

2.3 范围

如第2.1节所述，信息安全管理实践的目的是“保护组织开展业务所需要的信息”。该信息可以在信息系统上存储和处理，但是同样可以将其记录在纸上，或通过语言传递。本实践与此类信息的保密性，完整性和可用性有关，而不论在何处以及如何存储和处理这些信息。尽管重点是信息，该实践同时也与服务管理全部四个维度有关。

每个组织必须定义其信息安全管理实践的范围，通常包括：

- IT系统与服务
- IT基础设施和平台
- 软件和应用程序

- 网络基础结构，包括：IT网络，语音系统，无线系统等
- 终端设备，例如电话，笔记本电脑和平板电脑，包括：所有硬件，固件，软件和应用程序
- 物联网设备，通常具有网络连接和处理能力，并且可能也有与物理世界进行交互的传感器和驱动器
- 物理基础设施，例如：建筑物，数据中心或制造设备
- 业务流程
- 人员，包括了解他们所产生的风险以及如何管理这些风险
- 作为服务提供、管理和支持的一部分的合作伙伴和供应商
- 数据和信息（无论是存储，处理还是传达的信息及其格式）。

在该范围中，信息安全管理实践应确保：

- 需要保护的资产应被识别
- 可能影响这些资产的风险应被识别和分析
- 采取适当措施管理这些风险
- 监控和持续改进到位，以确保信息安全风险持续地被适当管理。

部分信息安全管理实践的重要内容在其他实践指南中进行了描述。表2.2 中列出了这些内容，作为本实践的参考供获取。

表2.2 与其他实践指南中描述的信息安全管理实践相关的活动

活动	实践
与客户，赞助商，监管机构和管理主体的战略沟通	关系管理 组织变革管理
与用户的运营沟通	服务台
建立和维护与供应商的合同	供应商管理

设计和实施产品和服务	服务设计 软件开发和管理 基础设施和平台管理 服务验证和测试 部署管理 发布管理
监控，发现潜在的安全事件	监控和事态管理

2.4 实践成功要素

实践成功要素

需要为一项实践提供综合功能组件，以满足实践的目标。

实践成功要素（PSF）不仅仅是一项任务或活动，因为它包括服务管理全部四个维度的组件。活动的性质和实践中PSF的资源可能有所不同，但它们共同保障实践的有效性。

信息安全管理实践包括以下PSF：

- 开发和管理安全信息策略和计划
- 缓解信息安全的风险
- 执行和测试信息安全管理计划
- 将信息安全嵌入到服务价值系统的所有方面。

2.4.1 制定和管理安全信息策略和计划

组织制定并维护安全信息策略和计划，以维持所需的安全信息水平。这些计划适用于组织内的每个人，并且有可能涉及服务的使用者，以及供应商和合作伙伴。因此，应该在整个组织内，保持沟通并理解适用的策略和计划。

组织应该了解内部和外部信息安全需求，以制定和管理其策略和计划。应对这些需求如何影响组织的资源、产品、服务和实践，以及是否使用了正确的信息安全控制进行评估。这些活动需要持续执行；

由于信息安全要求和组织环境的性质不断变化。应在基于时间间隔和基于事态的基础上，持续审查需求的变化以及策略和计划的充分性。应基于这些审查来启动改进。

信息安全管理政策和计划可能涉及以下方面：

- 整体信息安全管理实践方法
- 使用和滥用IT资产
- 访问控制
- 密码控制
- 沟通和社交媒体
- 恶意软件防护
- 信息分类
- 远程访问
- 供应商访问组织的信息和资源
- 知识产权
- 记录管理和保留
- 个人数据保护
- 其他信息安全相关因素。

为了确保信息安全的有效管理，组织可以建立遵循相关标准（例如ISO / IEC 270012）的正式信息安全管理体系。

2.4.2 缓解信息安全的风险

信息安全管理实践包括信息安全风险的识别，分析和管理。

信息安全风险的识别包括识别服务价值系统的范围内的所有资产，然后识别这些资产的风险。威胁和脆弱性评估，架构和设计审查以及许多其他技术都可以支持风险识别。

信息安全风险的分析包括确定每个信息安全风险的可能性以及该风险的潜在影响。提供的数据可以评估成本、收益以及潜在控制的ROI。

信息安全管理包括定义和管理控制，这些控制管理着可能影响信息安全的多种多样的风险。这是与风险管理和其他针对风险的实践（例如容量和性能管理，可用性管理和服务连续性管理实践）一起执行

的。商定的信息安全控制通常作为其他实践的一部分来实施，例如服务设计，软件开发和管理，基础设施和平台管理，架构管理，服务请求管理，持续改进，劳动力和人才管理，具体取决于控制的性质。

既定的策略和计划应驱动行为并实施控制以保持以下各项之间的平衡：

- 预防措施–确保不会发生安全事件
- 检测–快速可靠地检测无法避免的事件
- 纠正–在发现事件后从事件中恢复。

如果风险分析表明服务上的影响更早且更大，则应采取更多的预防措施。如果最初的影响较小，并且很久后才会进一步发展，则采用更经济有效方法投入到检测和纠正对策。

控制可能包括服务管理四维模型任何内容，例如：

- 组织和人员控制，例如培训，策略或职责分离
- 价值流和流程控制，例如备份，补丁管理或同行评审
- 信息和技术控制，例如防火墙，加密或防病毒软件
- 合作伙伴和供应商控制，例如合同要求，流程审核或第三方认证。

选择信息安全对策时，应评估每个选择的有效性和效率。信息安全的对策有效性和效率必须得到持续控制和验证。

2.4.3 演练和测试信息安全管理计划

经验表明，未经测试的计划根本无法正常工作。因此，测试是整个信息安全管理实践的关键部分。这是确保计划和控制在实践中工作的唯一方法。

信息安全计划和控制应当被测试，以改进它的可读性和可用性。常规测试将发现缺陷和失效。这些发现可用于更新信息安全的计划和控制。

应该在计划的时间间隔内，以及策略、计划和控制发生重大变化时进行演练。信息安全事件的影响越大，演练应该越频繁。

2.4.4 将信息安全嵌入到服务价值系统的所有方面

信息安全管理实践应当被嵌入到服务价值系统的每一个部分中。

2.4.4.1 指导原则

使用ITIL 指导原则时，考虑使用本实践是非常重要的。例如：

- 聚焦价值：价值可以通过信息质量中的改进来实现
- 协作和提升可视化：高层还会考虑信息的保密性。

2.4.4.2 治理

治理对于有效的信息安全管理实践至关重要。甚至最小的组织都应当针对以下内容建立本实践的治理：

- 确立组织对本实践的态度
- 定义本实践的高层需求
- 将高层需求传递给管理层
- 监视组织以确保满足这些需求。

2.4.4.3 服务价值链和价值流

每个价值流应包括适当的信息安全管理实践活动。通常，它们将被嵌入到价值流的多个步骤以及服务价值链的多个点中。例如，考虑一个价值流，它创建了一个新的或经过重大变更的服务：

- 确认并记录服务需求（契动）
  - 此步骤将包括记录对信息安全的服务需求
- 决定是否对新的服务进行投入（计划）
  - 在此步骤中，考虑可能对组织造成风险的信息安全事项
- 设计新服务满足客户需求（设计和转换）
  - 此步骤将包括设计和架构，以满足安全需求
- 构建，配置或购买服务组件（获取或构建）
  - 每个组件都需要被构建，配置或指定以满足安全需求
- 部署服务组件以准备启动（设计和转换）
  - 部署应该是安全的，以确保组件没有被篡改

- 向客户和用户发布新的服务（交付和支持）
- 用户和IT人员需要进行培训，包括安全培训，作为发布的一部分。

2.4.4.4 实践

每个实践都需求包含信息安全管理的很多方面。这可能与服务管理四维模型某项有关。

通过实践定义的流程需要包含此实践的活动。例如，部署流程需要包括检查以确保软件组件不被篡改。

实践定义的角色需要包括此实践的技能。例如，软件开发人员可能需要具备满足已定义的安全标准的软件设计能力。

实践使用的信息和技术必须满足安全需求，并且通常需要嵌入安全措施。例如，事件管理实践中用于信息交换的工具可能需要保密，因此工作人员只能看到其所在组织的事件，而不能看到其他组织的事件。

支持一项实践的合作伙伴和供应商必须满足组织的信息安全需求。例如，提供服务连续性安排的合作伙伴，需要确保其员工不能使用作为连续性测试的一部分而提供给他们的数据。

2.4.4.5 持续改进

与其他所有实践一样，信息安全管理实践也需要持续改进。在IT服务面对的威胁和依赖程度逐步增长的情形下，不断监视并改进信息安全至关重要。

所有改进活动，即使是那些没有特定信息安全管理实践内容，也应评估其对信息安全造成的潜在影响。该评估作为惯例应成为任何改进活动的一部分。

2.5 关键指标

应在每个实践所贡献的价值流的上下文中，评估ITIL实践的效益和绩效。与任何工具的绩效一样，只能在其所应用的上下文中评估该实践的绩效。然而，工具在质量方面差异很大。这些差异定义了工具根据其用途被使用时的潜力或性能。有关指标，关键性能或绩效指标（KPI）以及其他可以帮助实现此目标的技术的进一步指南，请参见度量和报告实践指南。

信息安全管理实践的关键指标已列入到其PSF。它们可以用作价值流上下文中的KPI，以评估实践对这些

价值流的效果和效率的贡献。表2.3 中给出了一些示例。

表2.3 实践成功要素的关键指标示例

实践成功要素	关键指标
制定和管理安全信息策略和计划	带有明确记录的信息安全要求的产品和服务的百分比 带有书面信息安全计划的产品和服务的百分比 定期更新信息安全计划的规则
缓解信息安全的风险	已执行分析和评价的信息安全风险的数量和百分比 通过实施控制将残留的风险降低到可接受的水平的信息安全风险的数量和百分比存在风险
演练和测试信息安全管理计划	在过去12个月中经过测试的信息安全管理计划的数量和百分比 测试信息安全管理计划后确定的改进活动数
在服务价值系统的所有方面都嵌入信息安全	治理主体在过去三个月中至少讨论过一次信息安全管理 包含信息安全特定步骤和活动的价值流的数量和百分比 在信息安全的流程和角色定义中包括特定步骤和活动的实践次数和百分比 包含安全评估的改进活动的数量和百分比

将指标正确汇总到复杂的指标中，将使数据更易于用于正在进行的价值流的管理，以及用于信息安全管理实践的定期评估和持续改进。没有单一的最佳解决方案。指标基于整体服务战略和组织的优先级，以及实践所贡献的价值流目标。

3 价值流和流程

3.1 价值流量贡献

像任何其他ITIL 管理实践一样，信息安全管理实践也有助于多个价值流。重要的是要记住，价值流永远不会由单个实践形成。信息安全管理实践与其他实践相结合，可以为消费者提供高质量服务。信息安全管理实践为服务价值链的所有活动做出了贡献。图3.1 中显示了信息安全管理实践对服务价值链的贡献。

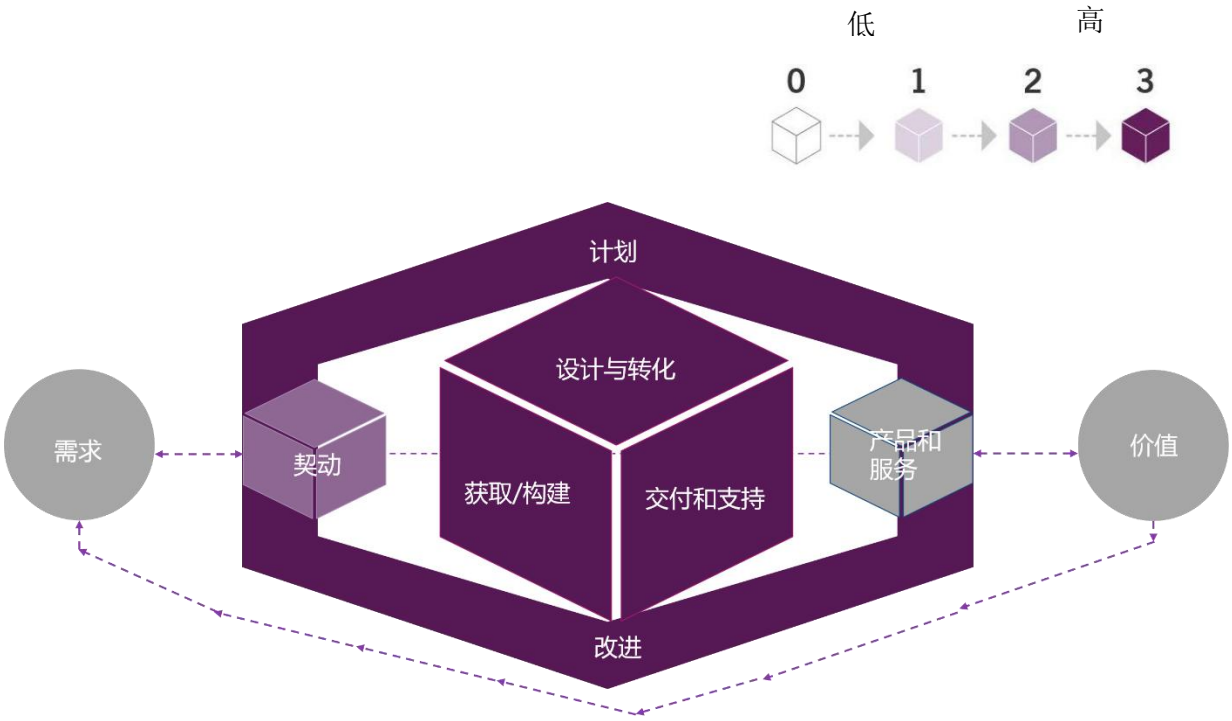

图3.1 信息安全管理实践对价值链活动的贡献热力图

3.2 流程

每个实践可能包含一个或多个流程和活动，它们对于实现该实践的目标可能是必需的。

定义：流程
一组相互关联或交互的活动，可将输入转换为输出。流程接受一个或多个定义的输入，并将其转换为定义的输出。流程定义动作的顺序及其依赖。

许多信息安全管理实践活动被嵌入到其他实践的流程中。例如：

- 将安全设计为新的和更改的IT服务是服务设计实践的一部分
- 将安全控制集成到应用程序中是软件开发和管理实践的一部分
- 确保人员使用服务前被授权，同时也是服务请求管理一部分。

信息安全管理实践构建了两个流程：

- 安全事件管理
- 审计和评审。

3.2.1 安全事件管理

安全事件有很多不同的类型。范围从单个客户设备受病毒影响，到对国家基础设施造成严重损害，或严重破坏高度敏感信息的攻击。

按照ITIL 事件管理实践指南中描述的事件处理和解决流程的规定，通常以与任何其他事件相同的方式来管理轻度安全事件。更严重的安全事件可能需要专业的管理，它可以基于本文件描述的流程。

每个组织应该定义一个标准，以确定事件是否需要专业的安全事件管理，或者可以使用常规事件处理和解决流程进行管理。

该流程包括表3.1 中列出的以下活动，并将以下输入转换为输出。

表3.1 安全事件管理流程的输入、活动和输出

关键输入	活动	关键输出
信息安全策略 服务和资产信息 监控和事态工具 安全事件和事态管理（SIEM）工具 从服务台进行升级 已知的数据和应用程序的良好来源	准备 检测和报告分类和分析 控制和恢复 事件后活动	事件响应计划 供应商合同 事件通知监管机构，治理机构或其他相关方 恢复信息和服务 事件报告 改进建议

图3.2 显示了流程的工作流图

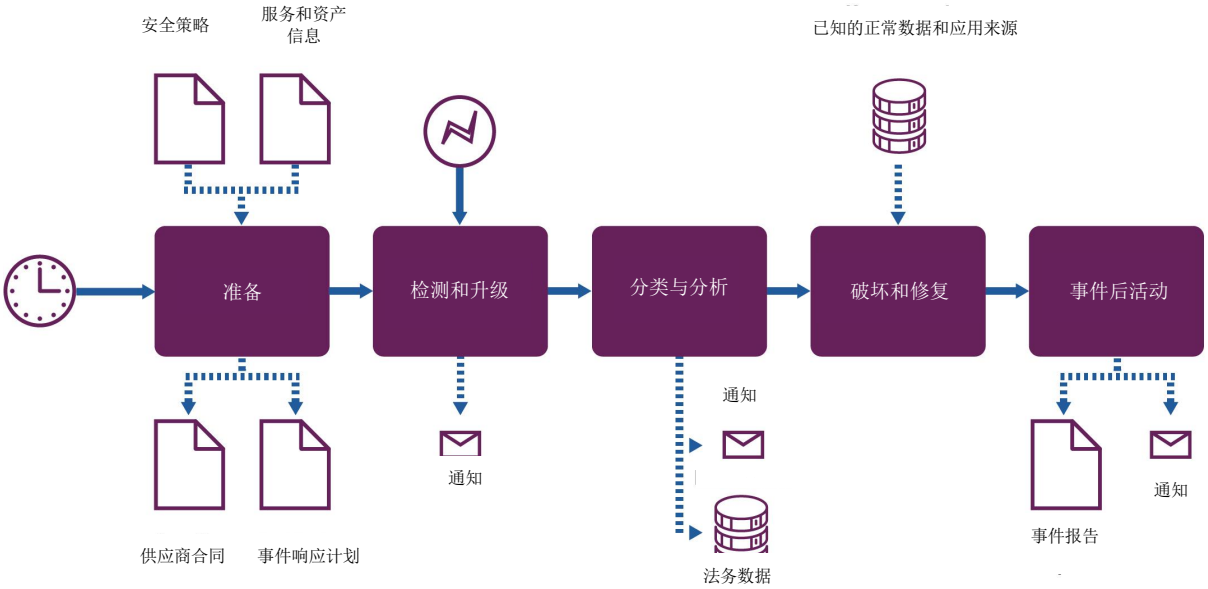

图3.2 安全事件管理流程的工作流

这些活动可能会由组织内的许多人以不同级别的形式执行。

表3.2 提供了流程活动的示例

表3.2 安全事件管理流程的活动

实现价值	例
准备	在安全事件发生之前，组织必须执行操作以为将来可能发生的安全事件做准备。这包括： 定义和传达安全事件管理的策略和程序 确定可能需要特定响应计划的关键服务和资产 允许在安全事件期间进行的沟通，包括与以下机构的沟通：治理机构，监管机构，执法机构，新闻界，客户，内部人员，用户，供应商以及任何其他受影响的利益相关者 定义如何报告安全事件和违规，以识别需要管理的威胁和漏洞，并记录特定场景的事件响应计划 让合作伙伴和供应商提供支持特定场景可能需要的产品和服务

	测试事件响应计划
检测和升级	信息安全事件可能是：由监控工具检测，受关联工具支持以及受安全事件和事态管理（SIEM）工具支持。事件也可由人员发现；可能会向服务台或安全事件响应小组报告，这取决于谁检测到事件以及事件的性质 根据特定的事件响应计划，将事件升级到适当的人员或团队。这可能涉及组建计算机安全事件响应团队（CSIRT） 如果需要，会将初始通知发送给适当的监管或治理机构
分类和分析	可能需要保留证据，以备将来使用司法程序。为防止污损，必须在进行任何分析之前收集司法数据 通过检查系统，端点，应用程序，日志文件等，可以确定安全事件的性质和严重性 如果需要，则在了解事件的性质和严重性后，可以将进一步的通知发送给监管机构或治理当局
遏制和恢复	受影响的系统和服务与Internet和/或组织的其余部分隔离。这样可以进行进一步的分析，同时限制了风险的进一步破坏 如果可能，则使用其他可选系统恢复服务 分析完成后，将关闭受影响的系统，擦除存储，并从知名且可靠的来源重建系统 如果可以在没有其他事件的威胁或最初事件造成进一步损坏的情况下运行业务，则认为流程已恢复
事件后活动	系统和服务被监视以保证威胁已被移除。进行经验教训分析以识别改进机会。事件报告完成创建并适当分享

3.2.2 审计和评审

审计和评审会定期执行并遵循时间表。重大事件或威胁评估或脆弱性评估的发现也可能触发它。

该流程包括表3.3 中列出的活动，并将以下输入转换为输出。

表3.3 审计和评审流程的输入、活动和输出

关键输入	活动	关键输出
业务流程信息 威胁评估信息 服务和资产信息 外部标准 当前控制 脆弱性评估信息	识别对业务，技术或威胁环境的变更 确定缺少的控制 评估控制效果 创建审计报告	改进建议 审计报告

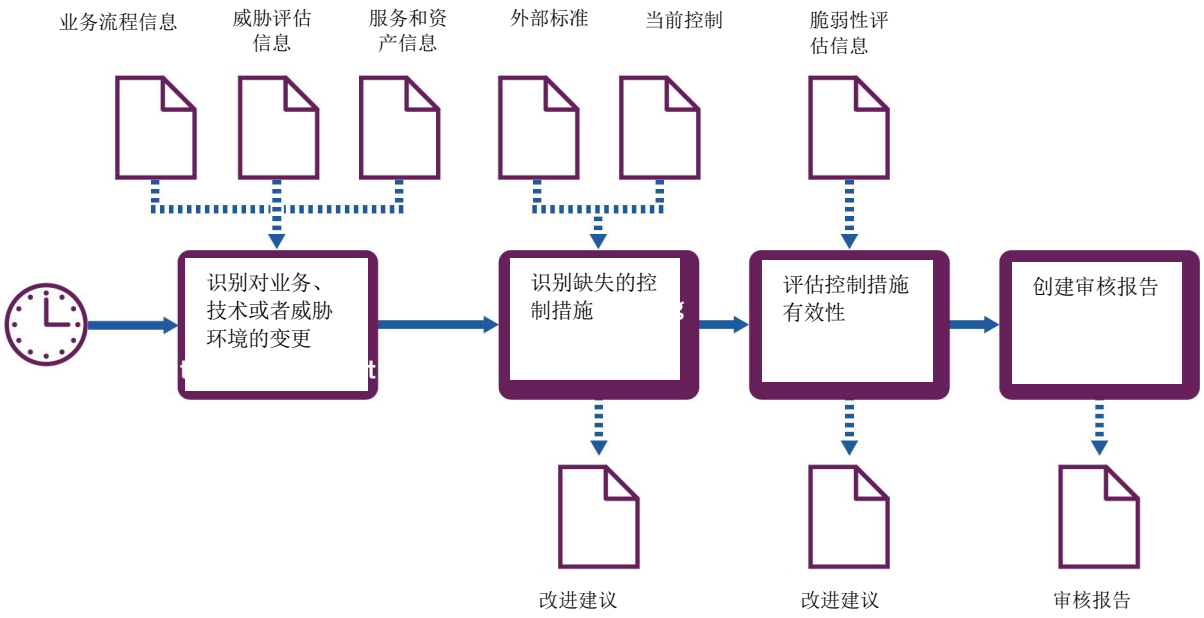

图3.3 审计和评审流程的工作流

图3.3 显示了流程的工作流图。

这些活动可能由内部或外部审核员执行。许多组织执行内部审计并实施改进。然后，外部审核员可以执行更正式的审计。

表3.4 提供了流程活动的示例

表3.4 审计和评审流程的活动

活动	示例
识别对业务，技术或威胁环境的变更	对业务流程进行评估，以识别影响信息安全需求的变更 对技术进行评估以识别新技术或已变更的技术，以及已过时的技术和技术相关漏洞中的变更。该评估考虑了组织所使用的全部技术，而不仅仅是信息技术（IT） 通过威胁评估识别对威胁环境的变更
识别缺失的控制	分析业务，技术和威胁环境，并确定了建议的控制。大多数组织使用标准（例如ISO / IEC 27002或NIST 800-53）作为初始的应采用的建议控制列表 脆弱性评估的输出也可能会识别缺少的控制 将推荐的控制列表与现有控制进行比较，并推荐进行改进
评估控制的有效性	评估每一项现存的控制，以此识别潜在脆弱性如何产生的。这些脆弱性与控制的范围相关，例如是否已在所有可能的地方部署。同时其与控制的配置相关，例如是否提供了适当等级的保护 评估效果的方法取决于控制的类型。例如： ● 使用脆弱性评估评估技术控制 ● 通过查看记录和员工访谈来评估策略和流程控制 ● 通过比较带有授权访问请求记录的目录信息评估访问权限 ● 通过测试员工知识来分析培训的价值 ● 确保第三方和供应商已通过正式的评估机构接受了适当的评价 ● 通过评估脆弱性评估的输出来识别无效的控制 根据此有效性评估的结果，推荐新的或改进的控制
创建审计报告	基于早期阶段的发现创建了审计报告。该报告包括可以提供给组织的治理主体的高级信息，以及有关新的和改进的控制的详细建议

4 组织和人员

4.1 角色，能力和责任

实践指南没有描述实践管理的角色，例如实践所有者，实践领导或实践教练。相反，他们专注于每个特定实践的专门角色。每个角色的结构和命名都可能因组织不同而不同，因此ITIL中定义的任何角色都不应视为强制性的或建议的。

请记住，角色不是职务。一个人可以担任多个角色，一个角色可以分配给多个人。

角色在流程和活动中被描述。每个角色都具有基于表4.1 中所示的模型的能力类型。

表4.1 能力代码和类型

能力代码	能力类型（活动和技能）
L	领导者，决策，授权，监督其他活动，提供激励和动机以及评估结果
A	管理员，分配任务并确定优先级，保留记录，持续报告并启动基本改进
C	协调者/沟通者，协调多方，维护利益相关者之间的沟通并开展宣传活动
M	方法和技术专家，设计和实施工作技巧，文件化步骤，流程咨询，工作分析和持续改进
T	技术专家，提供技术（IT）专业知识并进行基于专业经验的作业

4.1.1 首席信息安全官角色

许多组织都有负责信息安全管理实践的董事会成员。该角色通常称为首席信息安全官（CISO）。

CISO典型负责：

- 在了解组织业务战略的基础上，建立组织的总体信息安全战略，以及可能影响其的信息安全风险
- 确保组织对信息安全采取均衡的方法，提供足够的保护，而不会对开展业务的能力造成不利影响
- 有关安全信息的战略沟通给董事会和其他利益相关者例如监管机构，执法部门，媒体，客户，供应商和合作伙伴
- 制定信息安全政策和程序

- 监督负责安全信息所有其他方面的人员，包括：
  - 开发，测试和改进流程，尤其是安全事件管理
  - 选择，测试和部署安全产品，例如防火墙或防病毒软件
  - 为采购、开发，测试，部署定义标准和指南并持续管理具有安全影响的基础架构和应用程序，例如服务器，操作系统，SaaS产品，内部应用程序，中间件和客户设备
  - 运维活动，例如安全事态监控和安全产品例行检查。

4.1.2信息安全管理中涉及的其他角色

下表4.2 列出了信息安全管理实践中可能涉及的其他角色，以及相关的能力类型和特定技能。

表4.2 负责信息安全管理的角色示例活动

活动	负责角色	能力类型	特殊技能
安全事件管理流程			
准备	CISO 信息安全经理 安全分析员 CSIRT团队成员	LMCT	组织知识 策略和流程开发
检测和报告	安全分析师 技术分析师 服务台客服	CAT	识别安全事件并对其进行适当分类 组建团队并清晰沟通
分类和分析	CISO 信息安全经理 法医专家 安全分析师	TMA	业务优先级 取证数据的保存 对服务及其组件的技术理解 复杂系统和信息来源的

	技术分析师		分析
遏制和恢复	信息安全经理 安全分析师 技术分析师	TCM	对服务及其组件的技术理解 复杂环境下可选活动路径的评估与选择 多个利益相关者间的沟通与协调
事件后活动	CISO 信息安全经理 安全分析员	CTL	与多个利益相关者的沟通与协调 对服务及其组件的技术理解 改进机会的优先级
审计和评审流程			
识别对业务，技术或威胁环境的变更	CISO 信息安全经理	TMC	理解业务流程和优先级 理解当前和新兴技术 理解当前和正在出现的威胁
识别控制缺失	信息安全经理 信息安全审核员 安全分析员	TM	了解适用的安全标准，包括对安全控制的详细理解 对服务及其组件的技术理解分析能力

评估控制有效性	信息安全经理 信息安全审核员 安全分析员	TMC	了解适用的安全标准，包括对安全控制的详细理解 对服务及其组件的技术理解 沟通和审计技能分析能力
创建审计报告	信息安全经理 信息安全审核员 安全分析员	TCA	评估改进机会并确定其优先级 与广泛的利益相关者进行沟通，包括高级管理者

4.1.3 所有角色的安全能力

组织中的每个人都对信息安全管理实践负有责任。每个角色应该包括一些安全管理要求。那些了解信息安全管理实践功能的人可以：

- 通过遵循所有必需的策略，实施必需的控制以及通知和报告漏洞来防止信息安全事件和违规
- 通过通知和报告异常的行为技术，人员或供应商来检测信息安全事件和违规
- 通过在发生事件时遵循必需的流程和过程来更正安全事件和违规信息。

如果人员没有适当的技能，能力和动力，其也可以通过消极的方式为其中的每一项做出贡献。可以做很多事情来帮助确保组织中的每个人都为信息安全做出积极贡献。

4.1.3.1 安全意识培训

安全意识培训应帮助员工识别风险并采取适当的措施。培训通常包括以下问题：

- 用户身份验证，密码安全，多因素和生物特征识别
- 安全的Web浏览和社交媒体的使用
- 电子邮件，电话和其他通讯渠道的适当使用
- 端点安全，包括电话，平板电脑，笔记本电脑，可移动媒体的使用，个人设备等

- 远程和移动工作，包括使用公共Wi-Fi
- 社会工程学，网络钓鱼和身份盗窃
- 恶意软件，包括：病毒，勒索软件，键盘记录程序，广告软件，间谍软件等
- 高级持续性威胁
- 个人身份信息（PII）和数据隐私
- 信息分类以及对信息和其他资产的适当处理
- 安全事件报告和管理。

了解组织信息安全政策和控制的相关内容。安全意识应定期进行培训，尤其是新员工。一些组织每年进行一次进修培训，涵盖所有必需的材料。另外一些组织则提供更多的定期培训，这些培训每次仅涵盖部分材料，但一年的课程会包括所需的所有内容。

4.1.3.2 每个工作说明中的安全要求

每个工作说明应包括适当的安全活动。其中一些活动将是通用的，并且每个人都相同。其他将特定于组织内部人员拥有的角色。

4.1.3.3 定期强化安全信息

定期强化安全信息可确保安全意识在关键时刻处在员工头脑中的最前沿。这种强化可以采用海报，屏幕保护程序，电子邮件，管理简介或其他任何适合组织文化的方法。

4.2 组织结构和团队

在拥有专门IT部门的组织中，CISO的角色通常不在IT范围内，以确保实践的范围不仅限于IT。通常，CISO将有许多直接报告人员，他们能够制定策略和流程，执行安全审计并向其他人员提供安全信息指南。

许多组织都有专门的IT安全团队，该团队在整个组织中提供专业知识，但是在其他IT团队中拥有安全信息专业知识也很重要。例如：

- 服务架构师和服务设计师必须能够构架和设计安全的IT服务。他们必须拥有足够的知识和理解力才能自己完成大部分工作，即使他们可能需要专业安全工作人员的帮助。

- 应用程序开发人员必须能够编写安全代码。这需要理解安全编码指南以及应避免的常见错误。
- 服务台工作人员必须能够识别安全事件，并根据组织的安全策略和安全事件响应计划采取适当行动。
- 所有员工都必须知晓检测常见安全攻击的责任，并知道如何应对这些攻击。

5 信息和技术

5.1 信息交换

信息安全管理的效果取决于所使用信息的质量。该信息包括但不限于以下信息：

- 消费者的业务流程
- 服务的架构和设计
- 合作伙伴和供应商，以及它们提供的服务信息
- 有关信息安全的法规要求
- 市场上可能与信息安全有关的技术和服务
- 安全标准和最佳实践

该信息可以采用多种形式。实践的关键输入和输出在第3节中列出。

5.2 自动化和工具

在某些情况下，信息安全管理实践可以从自动化中受益。在表5.1 中提及的解决方案概述可能有效。

表5.1 信息安全管理活动的自动化解决方案

流程活动	自动化方法	关键功能	对实践有效性的影响
安全事件管理流程			
准备	知识管理工具和文档库	记录和沟通策略 程序和事件响应计划	中到非常高，取决于组织的大小和复杂性
	服务目录和配置管理数据库（CMDB）	识别关键服务和资产	很高
检测和报告	监控工具	检测可能的安全事	必不可少

		件	
	安全事件和事态管理（SIEM）以及相关工具	分析数据并检测可能的安全事件	中到非常高，取决于服务、应用程序和基础架构的复杂性
	入侵检测系统（IDS）和入侵防御系统（IPS）	检测攻击并通过自动操作做出响应	高
分类和分析	数据司法鉴定工具	保存必要的证据 法庭诉讼	可能从低到必要，取决于法律和法规环境
	SIEM或日志分析工具	分析安全事件	很高
遏制和恢复	备份和恢复工具	安全事态之后恢复数据	必要
	最终媒介库	恢复中使用的安全软件和应用程序源	很高
事件后的活动	持续改进登记册	记录和跟踪改进建议	高
	知识管理工具和文档库	记录和沟通事件信息和经验教训	中
审计和评审流程			
识别对业务，技术或威胁环境的变更	流程构建和流程构建工具	记录和交流业务流程	高
	服务目录和配置管理数据库（CMDB）	识别新技术或变更技术	高
识别缺失的控制	安全审计工具或问卷 脆弱性评估工具	识别可能需要的控制	高
评估控制有效性	安全审计工具或问卷 脆弱性评估工具	现有控制与良好实践比较	高

创建审计报告	知识管理工具和文档库	记录和交流审计报告	中
	持续改进登记册	记录和跟踪改进建议	高

6 合作伙伴和供应商

仅使用组织自己的资源来提供的服务很少见。大多数（如果不是全部）依赖于其他服务，这些服务通常由组织之外的第三方提供（请参阅ITIL Foundation 2.4 章节：服务关系模型）。由支持服务引入的关系和依赖在ITIL 实践指南的供方管理和服务级别管理中进行了描述。

合作伙伴和供应商可能会提供关键产品和服务组件。服务提供者需求与合作伙伴和供应商协商并同意信息安全的要求，以满足信息安全的需求。

合作伙伴和供应商还可能提供安全服务和解决方案的信息，例如：脆弱性评估，威胁评估，安全事件管理，提供安全相关基础架构或应用程序等。在这种情况下，他们还应该参与这些服务和解决方案的测试和审查。

如果供应商可以访问组织的网络，服务器或其他资源，这可能是安全违规行为。此风险需求将被识别和控制。通常，这是通过以下方式控制的：

- 网络隔离：防止供应商访问网络的更敏感部分
- 强身份验证和加密功能：防止供应商访问敏感的数据和系统
- 具有定期审核的合同条款：确保供应商理解对他们的期望并满足这些期望。

7 重要提醒

实践指南的大部分内容都应作为组织在建立和构建自己的实践时可能考虑的领域的建议。实践指南是组织可能考虑的主题目录，而不是答案列表。使用实践指南的内容时，组织应始终遵循ITIL 指导原则：

- 聚焦价值
- 从你所处的地方开始
- 基于反馈迭代推进
- 协作和提升可视化程度
- 通盘思考和工作
- 保持简单实用
- 优化和自动化。

有关指导原则及其应用程序的更多信息，请参见以下内容的第4.3节。

ITIL®Foundation：ITIL 4版。