信息安全管理

ITIL®4 实践指南

AXELOS.com

申明：

- 本文档由长河（微信achotsao）在机译的基础上经初步整理分解，精细化翻译工作正由ITIL先锋论坛组织的ITIL专家团队进行，预计到2020年年底之前全部完成。需要下载最终翻译版本请关注微信公众号：IT管理精英圈，或访问www.itil4hub.cn或www.itilxf.com。
- ITIL先锋论坛专家团队只是只是进行了这些著作的语种转换工作，我们并不拥有包括原著以及中文发行文件的任何版权，所有版权归Axoles持有，读者在使用这些文件（含中文翻译版本）时需完全遵守Axoles和TSO所申明的所有版权要求。

内容

1 关于本文件

本文档为信息安全管理实践提供了实用指南。它分为五个主要部分，内容包括：

- 有关实践的一般信息
- 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
- 用于实践的用于合作伙伴和供应商的注意事项。

1.1ITIL®4 鉴证方案

本文档的选定内容可作为以下课程的一部分进行检查：

- **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 一般信息

2.1 目的和描述

关键信息

信息安全管理实践的目的是保护组织进行业务所需的信息。这包括了解和管理保密性，完整性和可用性信息的风险，以及信息安全的其他方面（例如身份验证和不可否认性）的风险。

信息安全变得越来越重要，但又困难重重。信息安全管理实践在数字化转型的背景中越来越重要。这是由于数字化服务在各个行业中的增长，其中安全信息泄露可能会对组织的业务产生重大影响。云解决方案的广泛使用以及与合作伙伴和服务消费者的数字化服务一起使用的集成产生了新的关键依赖性，而控制的信息收集，存储，共享和使用方式的能力有限。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资。但是，组织之间缺少集成和一致性会产生新的漏洞，需要理解和解决。信息安全管理实践与其他规范（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更广泛的安全管理的专门分支。在服务经济中，每个组织的业务都是由服务驱动并具有数字功能。由于安全管理更加关注数字化服务和信息的安全，因此这可能导致学科的联系更加紧密。如果数字化转型消除了“ IT 管理”和“ 业务管理”之间的边界，则集成既可能又有用。（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保密性，完整性和可用性进行业务所需的信息，并带有一些活动和控件来保留这些特性。此外，信息安全管理实践通常与身份验证和不可否认性有关。

定义：保密性

防止信息泄露给未授权实体或将其提供给未授权实体。

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其机密保持秘密，并且不要滥用其个人信息或业务信息。

定义：可用性[1]

信息的特征，确保可以在需要时使用它

如果该信息在需要的时间和地点不可用，则组织无法执行其业务。

可用性管理实践考虑了服务可用性的许多方面。但是，信息安全管理实践主要与可用性有关。

定义：完整性

确保信息准确无误，并且只能由授权人员和活动进行修改

定义：身份验证

验证出现或声称是真实的特性或属性实际上是真实的。

不正确的信息可能比根本没有任何信息更糟。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。例如：

- 用户名和密码通常用于对人员进行身份验证，尽管通常首选使用生物特征识别和安全令牌的更严格的身份验证。
- 网站可以使用证书和加密来提供身份验证。

定义：不可否认

提供不可否认的证据，证明发生了涉嫌事态或执行了涉嫌性能或绩效，并且此事态或性能或绩效由特定实体执行了

自从IT系统和服务存在之前，就已经在业务事务中使用了不可否认性。传统上，将使用签名，如果需要更高级别的证明，则可能需要对该签名进行公证。信息安全依赖不可否认性，因此可以进行交易。这对于保留完整性信息至关重要。

2.2.2 资产，威胁，威胁参与者和漏洞

定义：资产

资产是具有价值到组织的任何东西。

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保护资产，以便组织可以执行其业务。

[1]此定义不同于可用性管理实践所使用的定义。服务可用性的定义与信息可用性的定义不同。

定义：

威胁是任何可能在资产上带有负影响的潜在事态。

威胁演员是构成威胁的任何人或组织。

脆弱性是资产或控制中的任何弱点，均可被威胁利用。

这些术语的相关关系如下：威胁参与者利用漏洞在资产上拥有影响。

2.2.2.1 威胁和脆弱性评估

威胁评估用于识别潜在威胁，因此组织可以采用适当的性能或绩效。该评估可能涉及查看有关组织先前受到的攻击，有关其他类似组织的近期攻击的历史信息，或者只是预测将来可能出现的潜在威胁。威胁评估的输出是组织需求在其规划中要考虑的威胁列表。当规划发生变化时，可以定期进行威胁评估，并作为检查。

脆弱性评估用于识别特定环境，服务或配置项中的漏洞。通常，这涉及编译潜在漏洞列表，并使用工具对环境中的每个组件进行测试验证，以查看脆弱性是否存在。脆弱性评估可以定期进行，也可以在部署期间检查基础架构或应用程序。有许多工具可以支持脆弱性评估，许多供应商可以将脆弱性评估为服务。

2.2.3 风险管理条款

信息安全管理实践利用了几个风险管理术语和概念。风险管理实践中也描述了这些术语。

风险管理术语在表2.1中定义。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，或使其更难以实现目标的事态。它也可以定义为成果的不确定性，并且可以在背景中用于测量阳性结果和阴性结果的概率。
控制	管理风险，确保实现业务目标或遵循流程的方法。
风险处理	处理风险采取的措施。风险处理选项为： 风险避免：通过不执行危险的实现价值来防止风险 风险修改：实施控件以降低风险的可能性或影响 风险共享：通过将一些风险传递给第三方来减少影响 风险保留率：故意决定接受风险，因为它低于可接受的阈值（并且在组织的风险胃口之内）。

剩余风险	控件应用程序之后保留的风险

2.3 范围

如第2.1节所述，信息安全管理实践的目的是“保护组织进行业务所需的信息”。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，或通过语音传达。此实践与该信息的保密性，完整性和可用性有关，无论在何处以及如何存储和处理该信息。尽管重点是信息，但该实践与所有服务管理四维模型有关。

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，无线等。
- 客户设备，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相互作用的传感器和执行器
- 物理基础设施，例如：建筑物，数据中心或制造设施
- 业务流程
- 人员，包括了解他们构成的风险以及如何管理这些风险
- 参与提供，管理或服务支持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：

- 确定需要保护的资产
- 识别和分析可能影响这些资产的风险
- 采取适当措施管理这些风险
- 监控和持续改进到位，以确保继续适当地管理安全信息风险。

信息安全管理实践的一些重要方面在其他实践指南中进行了描述。表2.2中列出了这些内容，以及对可以找到它们的实践的引用。

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

实现价值	实践
与客户，赞助商，监管机构和治理主体的战略沟通	关系管理 组织变革管理
运行的与用户的通信	服务台
与供应商建立和维护合同	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，以检测潜在的安全事件	监控和事态管理

2.4 实践成功因素

实践成功因素
实践的复杂职能型组件，是实践实现其目的所必需的。

实践的成功因素（PSF）不仅仅是一项任务或实现价值，因为它包括所有服务管理四维模型的组件。活动的性质和实践中PSF的资源可能有所不同，但它们共同确保实践有效。

信息安全管理实践包括以下PSF：

- 开发和管理安全信息政策和计划
- 缓解信息安全的风险
- 行使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政策和计划

组织制定并维护安全信息政策和计划，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，并且可能涉及服务的消费者，供应商和合作伙伴。因此，应在整个组织上保持认知以及对适用政策和计划的理解。

组织应该了解信息安全的内部和外部要求，以制定和管理其政策和计划。这些要求如何影响评估

然后可以执行组织的资源，产品，服务和实践，并实现安全控制的正确信息。该实现价值将连续执行；由于信息安全要求和组织的背景的性质不断变化。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
- 存取控制
- 密码控制
- 通信和社交媒体
- 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
- 信息安全的其他相关方面。

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 27001）的正式信息安全管理体系。2[1].

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这一点。

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，潜在控件的收益和ROI。

信息安全的管理包括定义和管理控件，这些控件管理影响信息安全可能存在的广泛风险。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。商定的信息安全控件通常作为其他实践的一部分来实现，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。

既定的政策和计划应驱动行为并实施控制措施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

[1] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en [2020年2月3日访问]

- 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较早且更大，则应采取更多的预防措施。如果最初的影响较小，并且需要更长的开发时间，则更经济有效的方法是投资检测和纠正对策。

控制可能涉及任何服务管理四维模型。例如：

- 组织和人员控制，例如培训，政策或职责分离
- 价值流和流程控件，例如备份，补丁管理或同行评审
- 信息和技术控件，例如防火墙，加密或防病毒软件
- 合作伙伴和供应商控件，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，应评估每个选件的效果和效率。信息安全的对策效果和效率必须得到持续控制和验证。

2.4.3 锻炼和测试信息安全管理计划

体验表明，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。

安全计划和控件的信息应按照改进的就绪性和能力进行测试。定期测试将导致发现缺陷和效率低下。然后，这些发现可用于更新安全计划和控制的信息。

应该在计划的时间间隔内以及政策，计划和控制措施发生重大变化时进行演习。信息安全事件的影响越大，练习应该越频繁地进行。

2.4.4 将信息安全嵌入到服务价值系统的所有方面

信息安全管理实践必须嵌入到服务价值系统的每个部分中。

2.4.4.1 指导原则

使用ITIL 指导原则时，务必考虑使用实践。例如：

- 聚焦价值：价值可以通过质量中的改进点来实现
- 协作和提升可视化程度：也是高级考虑信息保密性。

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。甚至最小的组织需求都可以将实践的治理建立为：

- 确立组织对此实践的态度
- 定义此实践的高级要求
- 将高级要求传达给管理
- 监视组织以确保满足这些要求。

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，它们将被嵌入价值流的步骤内以及服务价值链的多个位置。

例如，考虑一个价值流，它创建了一个新的或经过重大更改的服务：

- 确认并记录服务要求（契动）
  - 此步骤将包括记录服务对信息安全的要求
- 决定是否投资新的服务（计划）
  - 在此步骤中，请考虑可能对组织造成风险的信息安全
- 设计满足客户要求的新服务（设计和转换）
  - 此步骤将包括设计和架构，以满足安全的要求
- 构建，配置或购买服务组件（获取或构建）
  - 每个组件都需要构建，配置或指定以满足安全的要求
- 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
- 发布向客户和用户提供了新的服务（交付和支持）。
  - 用户和IT人员可能需要培训，包括安全培训，作为发布的一部分。

2.4.4.4 实践

每个实践需求都包含信息安全管理的各个方面。这可能与任何服务管理四维模型有关。

实践定义的流程可能需要包含此实践的活动。例如，部署流程可能需要包括检查以确保软件组件不受篡改。

实践定义的角色可能需要包括此实践的技能和能力。例如，软件开发人员可能需要具备满足定义的安全标准的设计软件的能力。

实践使用的信息和技术必须满足安全要求，并且通常需要嵌入式安全控件。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组织的事件，而不能看到其他组织的事件。

支持实践的合作伙伴和供应商必须满足组织的信息安全要求。例如，提供服务连续性安排的合作伙伴可能需要确保其员工不使用作为连续性测试的一部分提供给他们的数据。

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服务面临越来越多的威胁和依赖的世界中，至关重要的是不断监视改进信息和安全信息。

所有改进点活动，即使是没有特定信息安全管理实践内容的改进点，也应根据信息安全评估其潜

在的影响。该评估应该是任何改进点实现价值的例行公事部件。

2.5关键指标

应在每个实践所贡献的价值流的背景内评估ITIL实践的效果和性能或绩效。与任何工具的性能或绩效一样，只能在应用程序的背景内评估实践性能或绩效。但是，质量中的工具差异很大。这些差异定义了工具的潜力或根据其用途而有效的能力。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映射到其PSF。它们可以用作价值流的背景中的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 实践成功因素的关键指标示例

实践成功因素	关键指标
制定和管理安全信息政策和计划	带有明确记录的信息安全要求的产品和服务的百分比 带有书面信息的产品和服务的百分比安全计划 在限时的方式中更新信息安全计划
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 信息安全的数量和百分比存在风险，其中通过实施控制措施将残留的风险降低到可接受的水平
行使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点动作数
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信息安全管理 包含特定步骤的价值流的数量和百分比，以及有关安全的活动信息 在信息安全的流程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点活动的数量和百分比

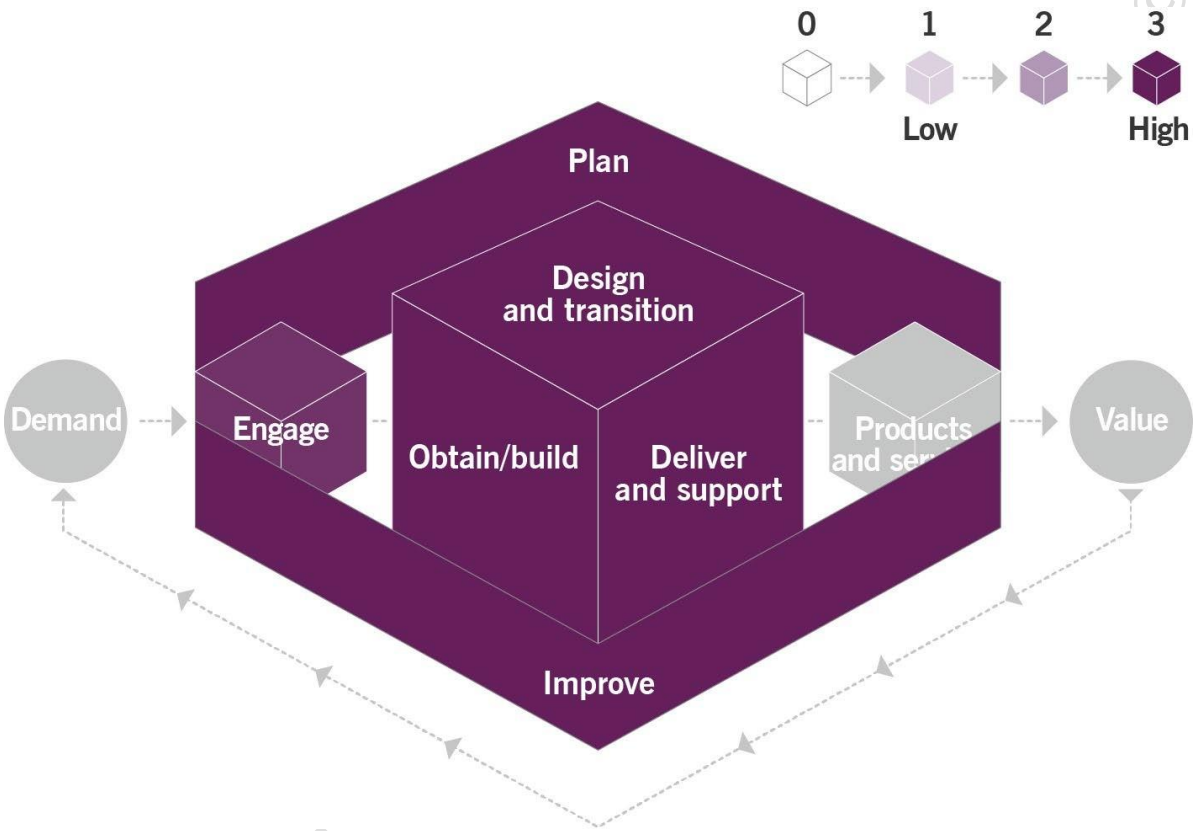
将指标正确汇总到复杂的指标中，将使数据更易于用于正在进行的价值流的管理，以及用于信息安全管理实践的定期评估和持续改进。没有单一的最佳解决方案。指标将基于整体服务战略和组织的优先级，以及实践所贡献的价值流的目标。

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。

图片3.1中显示了信息安全管理实践对服务价值链的贡献。



图片3.1 信息安全管理实践对价值链的贡献的热图活动

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的可能是必需的。

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性。

其他实践将许多信息安全管理实践活动嵌入到流程中。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
- 将安全控件集成到应用程序中是软件开发和管理实践的一部分
- 服务请求管理实践的一部分是确保在授予用户访问权限之前有权使用服务。

信息安全管理实践形成两个流程：

- 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。范围从受病毒影响的单个客户设备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家管理，它可以基于此处描述的流程。

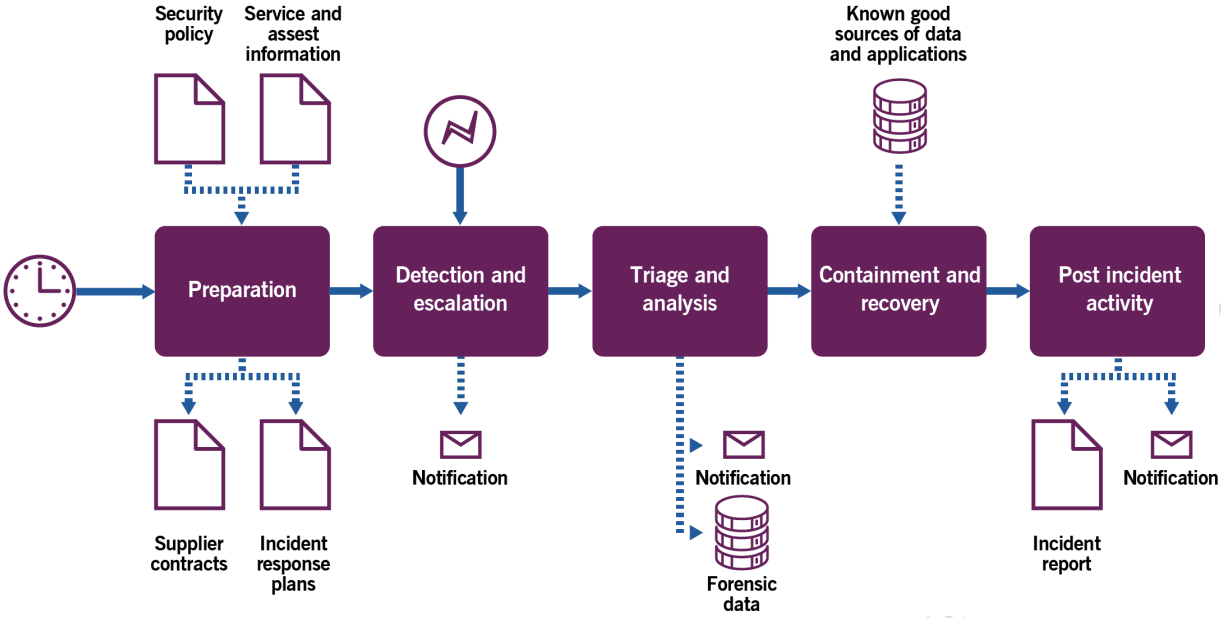
每个组织应该定义一个准则，以确定事件是否需要专家安全事件管理，或者可以使用常规事件处理和解决流程进行管理。

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 服务台的升级 数据和应用程序的已知良好来源	制备 检测和报告分类和分析收容和恢复-事件实现价值	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 事件报告改进点建议

图片3.2显示了流程的工作流程图



图片3.2 安全事件管理流程的工作流程

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
制备	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政策和程序 确定可能需要特定应对计划的关键服务和资产 同意在安全事件期间进行的通信，包括与以下机构的通信：理事机构，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。人们也可能发现事件；可能会向服务台或安全事件响应小组报告这些错误，这取决于谁检测到事件和事件的性质。

	根据特定的事件响应计划，将事件升级为适当的人员或团队。这可能涉及组装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法规或治理机构。
分类和分析	可能需要保留证据，以备将来使用。为防止污染，必须在进行任何分析之前收集法医数据。 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。
密闭性和恢复	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损坏。 如果可能，则使用其他系统的服务可能是恢复。 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原始事件造成进一步损坏的情况下执行业务，则认为流程已恢复。
事件后实现价值	监视系统和服务以确保已卸下威胁。进行经验教训分析以识别改进点机会。事件报告已创建并适当共享。

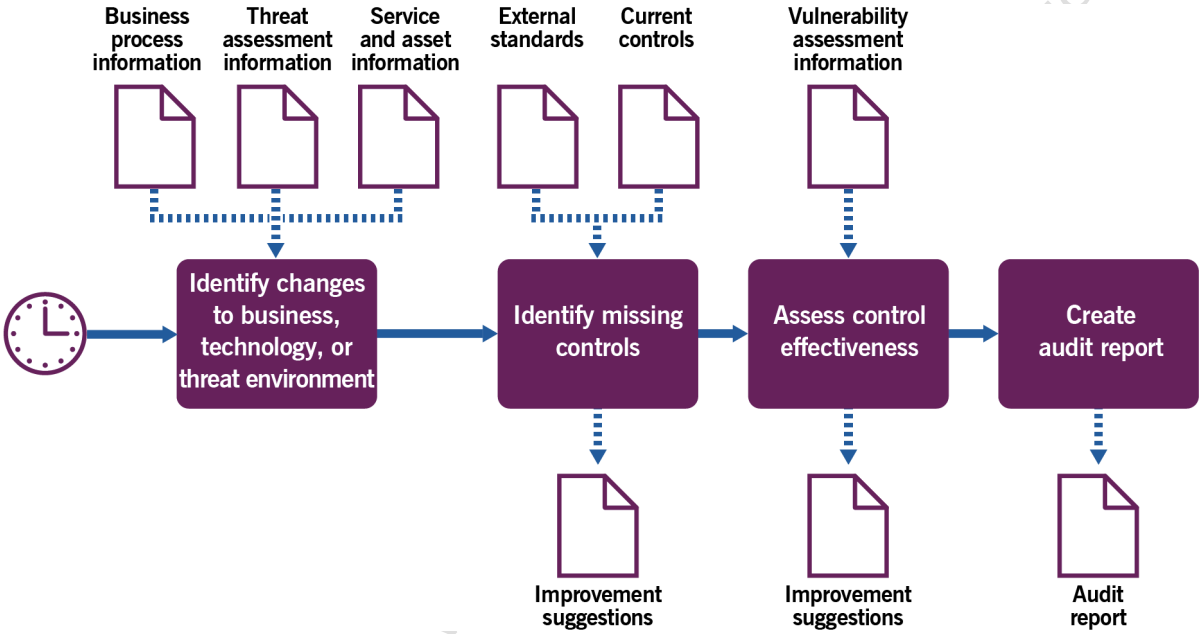
3.2.2 审计和评审

审计和审阅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（s）电流控制 脆弱性评估信息	确定对业务，技术或威胁环境的更改 确定缺少的控件评估控制效果创建审计报告	改进点建议审计报告



图片3.3 审计和评审流程的工作流程图片3.3显示了流程的工作流程图。

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核并实施改进。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

实现价值	例
确定对业务，技术或威胁环境的更改	对业务流程进行了评估，以识别可以使影响满足安全要求的更改。 对技术进行评估以识别新技术或已更改的技术，以及已过时的技术以及与技术相关的漏洞的更改。该评估考虑了组织使用的所有技术，而不仅仅是信息技术（IT）。 威胁评估标识对威胁环境的更改。
识别缺少的控件	对业务，技术和威胁环境进行了分析，并确定了建议的控件。大多数组织使用标准（例如ISO / IEC 27002或NIST 800-53）作为应采用的建议控件列表的开始。 脆弱性评估的输出也可能会识别缺少的控件 将推荐控件列表与现有控件进行比较，并建议进行改进。
评估控制效果	对每个现有的控制进行评估，以识别其实现方式中的潜在漏洞。这些漏洞可能与控制的范围有关，例如是否已将其部署到了应有的位置。它还可能与控制的配置有关，例如它是否提供适当的保护级别。 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。 ● 通过查看记录和采访人员来评估策略和流程控件。 ● 评审通过将目录信息与已授予访问请求的记录进行比较来访问权利。 ● 通过测试人员知识来分析价值的培训。 ● 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认证。 ● 通过评估脆弱性的输出来识别无效的控件评估。 根据此效果评估的发现，建议使用新的和改进的控件。
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件的详细建议。

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，实践主角或实践教练。相反，他们专注于每个实践的专门角色。每个角色的结构和命名都可能与组织和组织不同，因此ITIL中定义的任何角色都不应视为强制性的，甚至不建议使用。
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。

流程和活动的背景中描述了角色。每个角色都具有基于表4.1中所示的模型的能力概况。

表4.1能力代码和资料

能力代码	能力简介（活动和技能）
L	**领**导者决策，委派，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，进行中的报告并启动基本改进
C	**协**调员/沟通者协调多方，维护利益相关者之间的沟通并运行认知销售活动
M	**方**法和技术专家设计和实施工作技术，文档编制程序，有关流程，工作分析和持续改进的咨询
T	**技**术专家提供技术（IT）专业知识并进行基于专业知识的任务

4.1.1 安全首席信息官角色

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员（CISO）。

CISO通常负责：

- 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，以及可能对影响造成威胁的信息安全
- 确保组织对信息安全采取均衡的方法，
  提供足够的保护，而不会对业务的传导能力造成不利影响
- 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
- 制定安全信息政策和程序
- 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
  - 为采购定义标准和指南，开发，测试，部署和正在进行的具有安全含义的基础架构和应用程序管理，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