事件管理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专家团队进行之中，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

本文档为事件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
- 参与实践的组织和人员
- 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。

1.1 ITIL®4 鉴证方案

本文的选定内容可以作为以下教学大纲的一部分进行检查：

- ITIL专家：创建，交付和支持
- ITIL专家：高速IT

有关详细信息，请参考教学大纲文档。

2 一般信息

2.1 目的和描述

关键信息

事件管理实践的目的是通过尽快恢复正常的服务运营来最大程度地减少负面的影响事件。

正常的服务运营通常是在服务级别协议（SLA）或服务质量规范的其他形式中定义的，这是服务提供者在内部达成的协议。规范可以包含比最初与客户达成的协议更多的质量准则。因此，事件管理实践包括恢复正常的运维服务和资源，即使服务使用者看不到它们的失效或偏差。在这种情况下，普通运维在配置项目（CI）或服务技术规范中定义。但是，如果没有记录的正常运维的规范，则可以使用专家意见评估状况的资源和服务。如果需要，可以使用事件管理实践来纠正有故障的资源或服务。

事件管理实践是服务管理的基本元素。服务的快速恢复是用户和客户满意度中的关键因素，服务提供者的信誉以及组织在服务关系中创建的价值。

2.2 术语和概念

事件

服务的计划外中断或服务的质量减少。

事件管理实践确保将计划外的服务不可用或降级的时间减至最少，从而减少对用户的负面影响。有两个主要因素可以实现这一点：早期的事件检测和快速恢复正常的运维。

借助高效，高效的流程，自动化和供应商关系以及技术精湛且积极进取的专家团队，可以快速发生检测和解决事件。服务管理四维模型的资源被合并以形成事件管理实践。

一些系统和服务演示了包括所谓典型事件在内的操作模式。这些可能与已知的错误相关，例如缺乏兼容性或不正确的用户行为模式。服务提供者通常将事件模型定义为优化处理重复事件或类似事件以及解决。应用程序经过验证和测试的解决方案可帮助快速，有效地解决事件，并且通常可以带来更好的结果。

定义：事件模型

对特定类型的事件的管理的可重复方法。

事件模型的创建和使用对于事件管理实践中的活动很重要。这将在第3节中进一步描述。

尽管有些事件在服务运营和消费方面的影响相对较低，但其他事件却给服务消费者和服务提供者带来了严重后果。这些被称为重大事件，需要特别注意。

定义：重大事件

具有重要业务影响的事件，需要立即协调的解决。

重要的业务影响并不是重大事件的唯一特征。例如，当有多个为高可用性设计的系统和服务时，单个故障不太可能导致严重的业务影响。故障将迅速且通常是自动检测并修复。重大事件通常与更高级别的复杂性相关。例如，如果多个看似微不足道的事件同时发生，则它可能会升级并在服务使用者上拥有影响。诸如此类的复杂事件需要对管理和解决采用特殊方法。实施模型来管理所有事件将是有益的，即使重大事件很少重复发生且通常具有不同的性质。重大事件的模型可能包括：

- 清晰的准则，以区分重大事件与灾难及其他事件
- 特别负责的协调员，有时也称为重大事件经理（MIM）
- 创建了一个专门的临时团队来调查和解决重大事件
- 其他专用资源（包括预算）；例如，与第三方专家进行紧急咨询或采购组件
- 特殊的调查方法（例如，全功能团队）
- 与用户，客户，监管机构，媒体和其他利益相关者进行通信的约定模型
- 评审和后续的活动达成一致的规程。

定义：变通方案

减少或消除事件或问题的影响的解决方案，而该解决方案尚未提供完整的解决。一些解决方法可以减少发生事故的可能性。

有时，可能找不到事件的系统解决方案。在这些情况下，服务提供者可以应用变通方案。

解决方法迅速将复原，服务更改为可接受的质量。但是，变通办法可能会增加技术债务，并可能在将来导致新的事件。问题管理实践可用于减少事件解决方法创建的技术债务。在许多情况下，了解事件的原因可以帮助找到最佳解决方案。

定义：技术债务

待办项的总返工是通过选择解决方法而不是需要更长时间的系统解决方案来完成的。

2.3 范围

事件管理实践的范围包括：

- 检测和记录事件
- 诊断和调查事件
- 将受影响的服务和配置项还原到约定的质量
- 管理事件记录
- 在整个事件中与相关的利益相关者进行沟通生命周期
- 审查事件并在解决之后对事件管理和实践进行服务改进。

尽管许多活动和责任领域仍与之紧密相关，但它们并没有包含在事件管理实践中。表2.1中列出了这些活动，以及对实践指南的引用。重要的是要记住，ITIL 实践指南仅仅是价值流的背景中使用的工具的集合，应视情况而加以必要的组合。

表2.1其他实践指南中描述的与事件管理实践相关的活动

实现价值	实践指南
调查事故原因	问题管理
与用户沟通	服务台
实施产品和服务变更	变更使能

	部署管理
	基础设施和平台管理项目管理
	发布管理
	软件开发和管理
监控技术，团队和供应商性能或绩效	监控和事态管理
改进倡议的管理	持续改进
的管理和实现 服务请求	服务请求管理
如果使用灾难，则恢复正常操作	服务连续性管理

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；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。

事件管理实践包括以下PSF：

- 及早发现事件
- 快速有效地解决事件
- 不断改进事件管理方法。

2.4.1 尽早发现事件

以前，实践通常是根据最终用户和IT专家的信息来注册大多数事件的。发包信息的这种方法仍被广泛使用，但是好的实践当前建议自动检测和记录事件。可以在事件发生后立即开始影响用户之前执行此操作。这种方法具有多种好处，其中包括：

- 较早的事件检测缩短了服务不可用或降级的时间。
- 初始数据的较高质量支持正确的事件响应和解决，包括自动解决，也称为自我修复。
- 用户仍然看不到某些事件，从而改进了用户满意度和客户满意度。
- 在解决与客户同意的服务质量之前，可以解决某些事件，从而改善感知到的服务和正式报告的服务质量。
- 与事件相关的成本可能会降低。

事件检测由监控和事态管理实践启用。这包括用于事态分类的工具和流程，用于将事件与信息事件和警告区分开。

自动检测到的事件可以自动，手动或部分自动地分类。零件自动分类是手动进行的，但基于系统提出的建议。使用数据可以从过去的事件，事件，已知错误和其他来源获得自动化的事件和检测并进行分类，这可以从机器学习解决方案中受益。

当不可能使用自动事件检测时，通常会在事件已经影响用户及其工作时检测到事件。即使这样，事件的报告和注册越早，效果越好。这可以通过推广负责任的服务的文化来实现。

用户之间的消费，包括鼓励在合理范围内报告可疑事件和行为，并容忍虚假报告。

2.4.2 快速有效地解决事件

该PSF对于事件管理实践和通用服务质量的成功至关重要。考虑到环境的复杂性，在检测到事件之后，应该有效地进行处理：

- 在简单的情况下，例如重复发生的事件和众所周知的事件，预定义的解决程序可能是有效的。这些可能包括自动解决或标准化的路由和处理（根据适当的预先约定的事件模型）。
- 在复杂的情况下，事件的确切性质未知，但支持团队熟悉系统和组件，并且组织可以获取专家知识，因此通常会将事件路由到诊断和解决的一个或多个专家组。有时，这可以帮助识别模式，并导致模型和/或解决方案将来可以应用于类似事件。
- 在非常复杂的情况下，很难或不可能定义专家区域和专家组，或者已定义的专家组找不到解决方案时，采用集体方法可能会有用。此技术称为全功能团队。

全功能团队

解决各种复杂任务的技术。在全功能团队中，具有不同专业知识领域的多个人员一起完成一项任务，直到清楚哪些能力最相关和最需要。

通常，全功能团队有助于降低复杂度，并可以切换到不太复杂的环境中使用的技术。但是，全功能团队通常适用于性质未知的重大事件。在这种情况下，与仍未解决的事件造成的损失相比，将大量专用资源集中在一起是成本的有效方法。

全功能团队不需要举行物理会议。建立计划后，专家可能会独自工作以完成实验，设计脚本，并使用其他工具来发现正在发生的事情。对于带有事件的契动，全功能团队使用正确的人员，而不是大量的人员。

在复杂情况下可以使用其他技术。例如，可以将专家分析替换或与一系列旨在使改进了解以下内容的安全的失败实验结合：

事件的性质。基于复杂度的决策框架[1]对于在高度变化的复杂环境中处理事件很有用。

无论复杂性如何，从事件处理的第一步开始，都要确认事件数据的质量是否较高。这在以下方面具有强大的影响力：

- 决策的正确性
- 服务的速度恢复
- 有效利用资源
- 找到并纠正根本原因的能力
- 机器学习的可能性和质量。

2.4.2.1 事件的优先级

事故应尽快解决。但是，参与事件解决的团队的资源是有限的，并且这些团队通常同时参与其他类型的工作。应该优先处理某些事件，以最大程度地减少对用户的负面影响。

- **任**务优先级任务相对于其他任务的重要性。具有更高优先级的任务应首先处理。优先级在待办项中所有任务的背景中定义。
- **优**先级性能或绩效选择无法在待办项中为所有任务分配资源时首先要处理的任务。

事件优先级划分有许多简单准则：

- 评估事件的影响和紧急度（以及调查和解决的时间限制）并不是优先事项。但是，此评价可用于确定优先级和其他重要的注意事项，例如估计执行工作所需的时间。
- 仅当存在资源冲突时才需要确定优先级。如果在时间限制内有足够的资源用于流程的每个任务，则无需进行优先级排序。
- 事件应在单个待办项中与其他任务（计划的和计划外的）一起等待处理。
- 优先级排序是一种将人员分配到团队的背景中的任务的工具。如果事件由多个团队处理，则将根据资源可用性，目标解决时间和估计的处理时间在每个团队中确定优先级。

[1] http://cognitive-edge.com/videos/cynefin-framework-introduction

- 资源可用性和估计的处理时间由团队定义。而且，可以将处理时间标准化以用于重复操作。目标解决时间可以由SLA和/或服务提供者的内部服务规范定义。影响，评估和完成时间（解决）可能会在变更时出现，因为支持团队会发现新信息。
- 可视化工具（例如看板和精益原理，例如在制品的限制）对于有效的优先级排序很有用。

这些规则适用于服务提供者的专业团队执行的所有类型的工作，无论计划内还是计划外。重要的是，在所有实践中，组织的服务管理活动涉及的所有人都应同意并遵循它们。

2.4.3持续改进事件管理方法

应当定期对事件进行定期检查，以征询事件管理实践的改进，效果和效率。有些事件在解决上需要单独的评审。这通常适用于重大事件，新类型的事件以及未及时解决的事件。但是，大多数事件不需要确认解决是否成功就不需要单独的评审。但是，每隔一定时间对事件管理记录进行一次概述将有助于确定改进点的积极经验和空间。在专业团队之间共享知识；确定新的事件类型；和改进或引入事件型号。

定期审查提供了使用事件管理实践分析涉众的满意度的机会。定期事件评审也是实践的持续改进和组织的产品和服务的关键。

关键信息

数据的重要性

有效的评审将始终需要数据；因此，重要的是要商定记录的要求。数据应该是：

- **并**行确切地知道什么时候做了什么对帮助持续改进很有用。这要求利益相关者在事态期间（而不是之后）更新事件记录。同样，准确的时间表可能对调查问题有用。
- **完**整的信息实现价值可以隐藏在一个简单的语句后面。例如，诸如“我们重新启动集群并在45分钟后观察到正常的职能”之类的语句可能隐藏了有用的细节。这可能意味着：“我们先重启服务器4，然后重启2，然后再重启3，然后发现服务器4（正常运行）已停止。我们检查了手册，然后重新启动了服务器2和4，然后重新启动了服务器1和3。所有服务器在10分钟后都在正确处理数据。
- **全**面描述为什么要使用性能或绩效与

描述性能或绩效本身。

2.5 关键指标

应该在每个实践所贡献的价值流的背景内评估ITIL惯例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的性能或绩效。但是，设计和质量的工具可能会有很大差异，这些差异定义了工具的潜力，或根据用途使用能力才有效。有关度量标准，关键性能或绩效指标（KPI）的其他指南以及可以帮助您解决此问题的其他技术，请参见度量和报告实践指南。

事件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2.2中给出了一些关键指标的示例。

在实践中，应将指标应用于特定的背景，例如事件的类型，服务，专家组或时间段。将指标正确汇总到复杂指标中，将使数据更易于用于正在进行的价值流的管理，以及用于事件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。度量标准将基于服务战略的整体和组织的优先级，以及实践所贡献的价值流的目标。

表2.2 实践成功因素的关键指标示例

实践成功因素	关键指标
尽早发现事件	事件发生到检测之间的时间 通过监控和事态管理检测到的事件百分比
快速有效地解决事件	诊断的事件检测和销售活动之间的时间诊断的时间 调动次数 事件总处理时间中等待时间的百分比首次解决速率

	满足约定的解决时间 具有事件处理功能的用户满意度和解决自动解决的事件 百分比 用户报告之前已解决的事件的百分比
不断改进事件管理方法	使用先前确定和记录的解决方案的事件分辨率的百分比 使用事件模型改进点的关键实践指标随时间推移解决的 事件百分比 事件的速度和效果指标之间的平衡 解决

3 价值流和流程

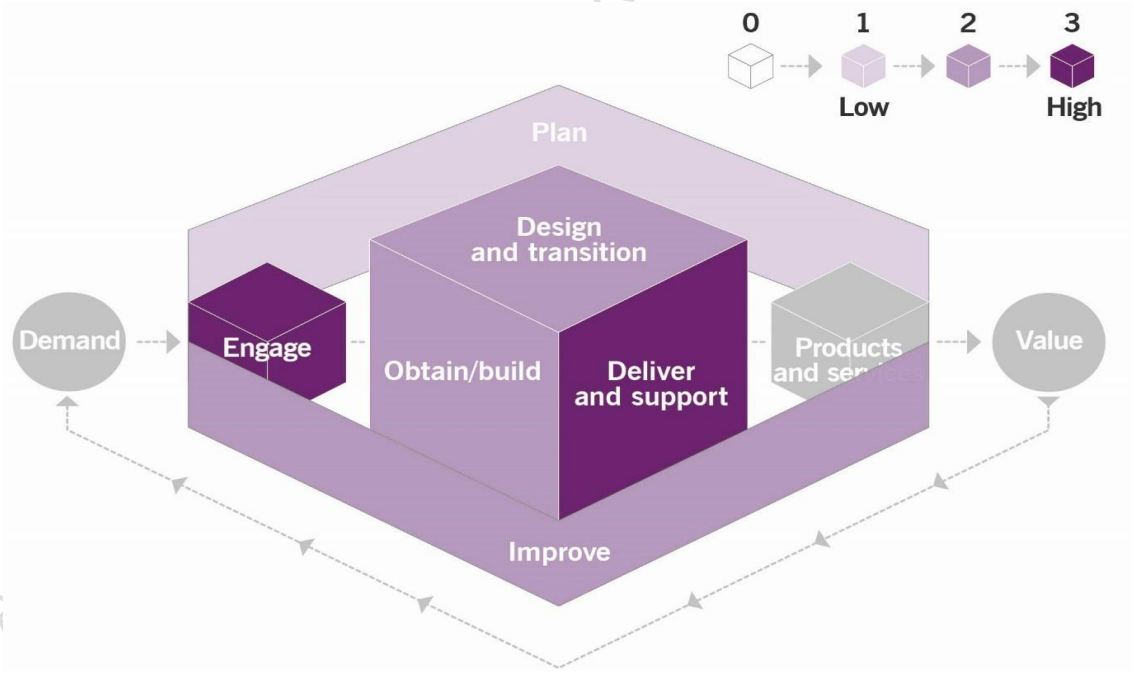
3.1 价值流量贡献

像任何其他ITIL 实践一样，事件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。例如，即使当价值流专注于事件解决时，也会涉及其他实践，例如服务台，监控和事态管理，服务配置管理，变更使能，供应商管理，基础设施和平台管理和软件开发和管理。

事件管理实践主要与在各种工作环境中恢复正常系统或服务运营有关。实践贡献的主要价值链活动是：

- 契动
- 交付和支持
- 设计和转换
- 改进
- 获取或构建。

图片3.1中显示了事件管理实践对服务价值链的贡献。



图片3.1 事件管理实践对价值链活动的贡献的热图。

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的可能是必需的。

> 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。

事件管理活动形成两个流程：

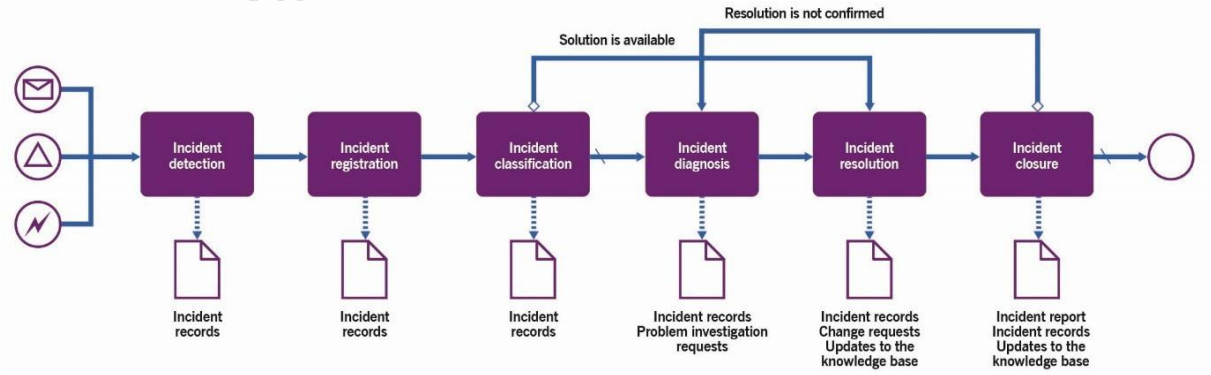
- **事**件的处理和解决该流程的重点是从检测到关闭的单个事件的处理和解决。
- **定**期事件评审该流程确保从事件处理和解决的课程中吸取教训，并确保持续改进事件管理的方法。

3.2.1 事件处理和解决

该流程包括表3.1中列出的活动，并将输入转换为输出。表3.1 事件处理和解决流程的输入，活动和输出

关键输入	活动	关键输出
监控和事态数据用户查询 配置信息IT资产信息服务目录 与消费者和供应商/合作伙伴的SLA 容量和性能或绩效信息 连续性政策和计划 信息安全政策和计划 问题记录 知识库	事件检测事件注册事件分类事件诊断事件解决事件关闭	事件记录 事件状况通信问题调查请求变更请求 事件报告 知识库恢复CI和服务的更新

图片3.2显示了流程的工作流程图。



图片3.2 事件处理和解决流程的工作流程

在整个流程中，应确保对每个事件拥有所有权。所有权可以在处理过程中和解决，流程的过程中转让，但是每个事件应该在任何时候对此负责。另外，只要事件的状况有变化，就应该更新利益干系人通信。

流程可能会有所不同，具体取决于事件模型。表3.2提供了两个事件型号（手动和自动）中的活动的示例，它们只是许多选项中的两个。它们旨在说明事件模型之间的差异。

表3.2 事件的活动和解决流程的处理

实现价值	手动处理用户检测到的事件	自动检测和处理事件
事件检测	用户检测到服务运营中的故障，并通过约定的通道与服务提供者的服务台联系。服务台代理执行用户查询的初始分类，确认该查询确实指的是事件。	事态被监控系统检测到，并基于预定义的分类被标识为事件。
事件注册	服务台代理执行事件注册，将可用的数据添加到事件记录。	已注册事件记录并将其与已检测到事态的CI关联。预定义的技术数据已注册。如果需要，将通知发送到相关技术专家。
事件分类	服务台代理执行事件的初始分类；这有助于鉴定事件影响，确定负责失败的CI和/或服务的团队，以及将事件与其他过去和正在进行的事件，事件和/或问题联系起来。 在某些情况下，分类有助于揭示了针对此类事件的先前定义的解决方案。	根据预定义的规则，将自动发现以下内容： • 事件关于服务和用户的影响 • 可用的解决方案 • 如果自动化解决方案无效或不可用，则负责事件解决的技术团队。

事件诊断	如果分类没有提供解决方案的理解，专家团队执行事件诊断。团队之间可能涉及事件的升级，或联合技术（例如全功能团队）。 如果由于配置项分配错误而导致分类错误，则应将此信息传达给负责配置控制的人员（请参阅服务配置实践指南）。	如果自动解决方案无效或不可用，则事件是上报给负责诊断的技术团队。团队之间可能涉及事件的升级，也可能涉及诸如全功能团队的联合技术。 如果自动化解决方案由于错误的CI关联而失败，则应将此信息告知负责配置控制的人员（请参阅服务）。配置实践指南）。

事件解决	找到解决方案后，相关专家团队将尝试按顺序或并行工作来应用它。可能需要启动变更。如果解决方案不起作用，则执行其他诊断。	如果有可用的自动化解决方案，则将对其进行应用，测试和确认。如果需要手动干预，则相关的专业团队将尝试应用它。可能需要启动变更。如果解决方案被证明不起作用，则附加诊断被执行。
事件关闭	成功解决事件之后，可能需要许多正式的关闭程序： • 用户确认服务恢复 • 解决成本计算和报告 • 解决价格计算和发票 • 问题调查启动 • 事件评审。 在完成所有必需的操作并相应地更新了事件记录之后，事件正式为已关闭。这可以由产品负责人，服务负责人，事件经理或服务台代理完成，具体取决于商定的事件模型。	如果自动解决方案证明有效，则事件记录将自动更新并已关闭。报告已发送给负责的技术团队。如果在先前的任何步骤中已将有关事件的信息传达给其他涉众，则还应该传达事件的关闭。

3.2.2 定期事件评审

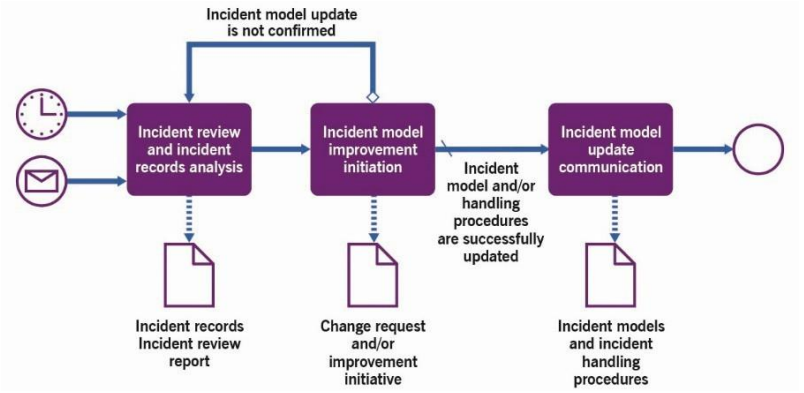
该流程专注于事件管理实践，事件型号和事件处理程序的持续改进。它可以定期执行，也可以由事件报告触发，该报告突出显示了低效率和其他改进点机会。取决于现有模型和程序的效果，可能会每两到三个月或更频繁地进行定期检查。

该流程包括表3.3中列出的活动，并将输入转换为输出。

表3.3定期事件的输入活动和输出评审流程

关键输入	活动	关键输出
当前的事件型号和程序	事件评审和事件记录分析	更新的事件型号
事件记录事件报告	事件模型改进点启动	更新了事件处理程序
政策法规要求	事件模型更新通讯	事件记录
配置信息IT资产信息		关于更新的事件型号和过程的交流
与消费者和供应商/合作伙伴的SLA		变更请求改进倡议事件
容量和性能或绩效信息		评审报告
连续性政策和计划		
安全政策和计划		

图片3.3显示了流程的工作流程图。



图片3.3定期事件评审流程的工作流程

表3.4提供了流程活动的示例。

表3.4 活动的定期事件评审流程

实现价值	例
事件评审和事件记录分析	事件经理与服务所有者和其他相关的利益相关者一起，对选定的事件（例如重大事件，未及时解决的事件或特定时期内的所有事件）执行评审。他们确定了事件模型和事件处理程序优化的机会，包括事件处理的自动化和解决。
事件模型改进点启动	事件经理使用持续改进实践的参与度注册要处理的改进倡议或启动变更请求（如果包括事件型号，过程和自动化）在变更使能实践的范围中）。
事件模型更新通讯	如果事件模型成功更新，则将其传达给相关的利益相关者。这通常由事件经理和/或服务或资源所有者完成。

4 组织和人员

4.1 角色，能力和责任

ITIL 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被视为强制性的，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 事件经理角色

在许多组织中，事件经理角色由专门人员执行，有时以事件经理的职衔进行。在其他组织中，事件经理的责任由负责与事件关联的CI，服务或生产的人员或团队承担；这可能是资源所有者，服务负责人或产品负责人。

该角色通常负责：

- 根据组织设计在组织或特定区域（例如区域，生产和技术）中协调事件处理
- 将人工工作与事件协调起来，尤其是涉及多个团队的事件
- 监控并审查处理和解决事件的团队的工作
- 确保在组织上有足够的认知事件及其状况
- 进行定期的事件审查，并开始对事件管理实践，事件模型和事件处理程序进行改进
- 开发组织在流程和事件管理实践方法方面的专业知识。

在某些情况下，组织可能会引入重大事件经理（MIM）的其他角色。该角色的职责与事件经理的职责相似，但专门用于重大事件。角色成为重大事件期间联系和协调的主要点。MIM通常具有更广泛的权限，并且可能具有用于主要事件管理的专用资源。

这些角色的能力概况是LCTA，尽管每种能力的重要性从实现价值到实现价值都不同。

4.1.2 事件管理活动中涉及的其他角色

表4.2中列出了事件管理活动中可能涉及的其他角色的示例，以及相关的能力概况和特定技能。

表4.2负责事件管理活动的角色示例

实现价值	负责角色	能力简介	具体技能
事件处理和解决流程			
Incident detection	技术专家用户	TC	了解事件的服务设计，资源配置和业务影响症状
事件注册	事件经理 服务台代理技术专家	在	我对IT服务有很好的了解管理(ITSM)工具和程序

Incident classification	事件经理服务台代 理商技术专家	TC	对服务设计，资源配置和业务影响的理解 对事件解决的要求和承诺有很好的了解 对事件模型的了解
Incident diagnosis	供应商 技术专家	TC	对服务设计，资源配置和业务影响的理解 事件模型，诊断工具，方法的知识 分析能力
Incident resolution	供应商 技术专家用户	T	了解事件所需的方法和过程解决
Incident closure	事件经理服务台代 理商技术专家	法案	对服务设计，资源配置和业务影响的理解 熟悉事件的要求和承诺解决
定期事件评审流程			
事件评审和事件记录分析	事件经理产品负 责人服务负责人 供应商	TCL	对服务设计，资源配置和业务影响的理解 的知识 事件的要求和承诺解决

			了解事件型号， 诊断工具，方法和分析技能
事件模型改进点启动	Incident manager Product owner Service owner	TMC	对服务设计，资源配置和业务影响的理解 熟悉事件的要求和承诺解决 事件模型，诊断工具和方法的知识 组织的知识 持续改进和变更使能实践
事件模型更新通讯	事件经理产品负责人服务台代理 服务负责人	钙	交流程序和工具的知识

4.2 组织结构和团队

事件管理实践不建议使用任何特定的组织模型。但是，组织结构会影响实践的执行方式，因为它涉及具有不同领域和专业水平的专家。分组专家的典型方法包括：

- 技术领域
- 生产/服务
- 领土
- 消费者类型。

组织的方法将有所不同，具体取决于组织的需求和资源。事件管理实践应该对其组织采取灵活的方法，必要时会涉及各种内部和外部团队的资源。

4.2.1 分层与扁平型团队结构

从历史上看，处理事件的团队具有分层或分层的结构，其中能力，专业知识和专业知识随每个级别而增加。它旨在以尽可能低的水平解决大多数事件，以降低成本。如果无法在当前级别解决事件，则将事件转移到更高级别或升级。在这样的团队中，升级事件的级别和清晰的过程之间存在明确的界限。不幸的是，这样的结构会限制协作和信息流动，导致解决时间延长。因此，对于优先级高事件，团队合作以促进快速的解决。

IT系统（例如自我修复系统）中敏捷方法的扩展和质量的变化要求更广泛地使用水平团队结构，而不是分层团队结构。更扁平的结构和相应的协作方法（例如全功能团队）代替了分层结构，以简化合作和免费的流动信息。此类变更的主要驱动力是拒绝刚性分层，而采用更具动态性，自组织性的协作代替它。

例

三层（L1，L2，L3）团队中的典型升级流程可以替换为以下内容：

- 用扁平的配对系统（或类似的系统）将L1替换为L2 升级，目的是将剩余问题的解决和流动更快地传输到L3
- L3的协作团队之间，以取代多次重新分配和/或对专家和冠军的过度依赖。

4.2.2 团队动力

事件管理实践是团队动态的基础，因为它们会影响支持运维的功能。经常出现以下问题：

- 事件在团队之间重定向
- 团队成员体验缺少自治和报告被其他人阻止的情况
- 文化盛行，当事件解决后，奖励单独的“英雄”。

这导致事件管理实践不同步，解决方案执行缓慢或根本不执行，士气下降，缺乏动力以及进入工作场所的竞争力不健康。此外，团队成员之间的信任也破裂了。DevOps和全功能团队之类的方法显示出鼓励积极使用文化所需的一些特征，尽管不必遵循这些方法来实现正确的团队动态。需要解决以下三个主要领域。

4.2.2.1 集体责任

如果解决事件是首要责任，那么团队中的每个人都将重点放在解决问题上。团队动力仅次于达成SLA或按时完成。改变这一点的第一步是将构建和文化共享给团队成员成功和失败的地方。责任分担的团队可能只有一个人看到事件到解决，但是应该鼓励他们与流程中的其他有经验的人一起学习。发生这种情况时，组织将受益于正常服务的快速恢复以及知识共享。

4.2.2.2 无罪文化

团队中应该没有责备的文化；否则，这将导致个人，团队和供应商之间的信任度下降。事件的调查和审查需要解决事件，解决和服务的恢复问题。如果事件的想法行不通，则必须鼓励其采取行动，而不必担心受到报应。

4.2.2.3 持续学习

团队成员需要分享他们从实验中学到的课程，以便他们可以学习改进。在许多环境中，尤其是外包比例较高的环境中，这可以证明是文化上的重大飞跃。

5 信息和技术

5.1 信息交流

事件管理实践的效果基于所使用信息的质量。这包括但不限于以下信息：

- 客户和用户
- 架构和设计的服务
- 合作伙伴和供应商，包括有关它们提供的服务的合同和SLA信息
- 规范服务提供的政策和要求
- 利益干系人满意度和实践。

该信息可以采用多种形式，具体取决于所使用的事件型号。实践的关键输入和输出在第3节中列出。

事件的详细信息是最重要的信息。这些通常包括：

- 信息来源
- 对生产，服务或CI的引用失败或在标准以下执行
- 受影响的用户或服务
- 性能或绩效的症状
- 当观察到症状时
- 症状开始之前，正确的运维的最后一次已知时间
- 是否应用了自动修复（如果没有，原因）
- 地域和虚拟位置
- 影响正常运行的性质和程度
- 可能受不良性能或绩效影响且当前运行正常的类似系统
- 导致症状观察的事件顺序。

事件管理实践期间将交换和记录的其他信息应包括以下详细信息：

- 调查（如果有）
- 每个性能或绩效，包括结果。

任何采取的措施都应记录在案，以产生准确的时间表。如果实时记录操作不现实，则文档应指定性能或绩效的启动和完成时间，以避免创建错误的历史日志。但是，如果客户可以通过门户查看信息，则最好捕获实时操作。在可能的情况下，动作注册应该是自动化的。

应提供事件记录，以使其遵循支持代理或专家的自然工作流程，并应包括表5.1中所示的数据。

表5.1 事件记录中包含的数据

领域	推荐内容	说明
事件标题（简短说明）	职能或流程以及观察到的故障或降级	带有清晰说明的解决方案搜索速度更快
用户	受影响的用户，已报告用户	
当前影响	文字说明对用户/ 客户工作流程的实际影响	创建背景以允许解析器组执行供应适当的解决方法或修复程序
未来影响	潜力文字说明 客户继续使用影响，而事件继续	创建背景以允许解析器 组到供应适当的解决方法 或修复
第一次症状的时间	监控或用户体验中的日期和时间	指出确定因果关系的那一刻
上次上架时间职能	验证职能正常的日期和时间	查明应在何时找到触发器事态（此信息是人为添加还是自动记录的，可能会影响可信度）
受影响项目的详细信息（职能，CI，流程）	资产ID号，应用程序和流程名称以及CI参考	专注于修正的工作
可比项目的详细信息不受影响（如果任何）	不受影响的资产ID号，应用程序和流程名称以及CI参考	缩小寻找原因
调查详细信息（如果有）	调查步骤和步骤结果	减少重复工作
分配给	拥有事件的个人或团体	

5.2 自动化和工具

事件管理实践应该是自动化的。在可行且有效的地方，可能涉及表5.2中概述的解决方案。

在某些情况下，对于特定事件类型，可以使用预定义脚本和场景对事件处理中的特定实现价值之后的所有活动和解决流程进行完全自动化。

请注意，事件管理实践中使用的自动化工具不仅可以包括适用于所有事件的组织范围内的工具，还可以包括针对特定事件型号定期产生的事件评审流程所创建的一些本地自定义工具和脚本。两者都应用于驱动自动化工作。

表5.2 事件管理活动的自动化解决方案

流程实现价值	手段 自动化	关键功能	实践的效果上的影响
事件处理和解决流程			
Incident detection	监控工具和事态相关引擎	早期的检测和事件关联，从而启动了事件管理实践	高
事件注册	用户查询管理和工作流程工具，以及协作工具	有效记录事件	高

Incident classification	用户查询管理和工作流程工具，协作工具，知识管理工具，配置管理工具以及基于机器学习的分类引擎	快速正确的分类和事件分配，已知解决方案的识别，重大事件的识别	非常高，尤其是在事件数量多的情况下

Incident diagnosis	分析和调查工具知识管理工具配置管理工具和协作工具	假设的快速正确定义和测试，多个专家/团队的有效协作	很高，尤其是在需要手动协作的复杂事件数量很高时
Incident resolution	远程管理工具，自动化的部署系统，和协作工具	快速纠正有故障的配置项并恢复服务	高，尤其是在偏远地区提供服务时
Incident closure	用户查询和工作流管理工具，以及协作工具	事件的快速而全面的概述生命周期	介质
定期事件评审流程			
事件评审和事件记录分析	协作系统，分析和报告系统以及调查工具	远程协作，事件数据分析和用户调查数据分析和报告	中到高，尤其是对于大量事件
事件模型改进点引发	工作流程系统和待办项工具	倡议的正式注册	中低
事件模型更新通讯	通信系统和协作系统	向受影响的团队传达更新	中到高，尤其是当组织很大且更新数量大时高

6 合作伙伴和供应商

仅使用组织自己的资源提供的服务很少。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：服务关系的ITIL 4 Edition的ITIL 4版）。服务设计，架构管理和供应商管理的实践指南中描述了由支持服务引入的关系和依赖性。

事件模型应定义XTC83011 解决如何涉及第三方以及组织如何确保有效的协作。这将取决于产品，服务和价值流的架构和设计解决方案。但是，支持这些解决方案的事件模型的优化将涉及事件管理实践。通常，在为事件选择了正确的模型之后，在事件，诊断，解决和评审期间，还需要第三方依赖的考量。

定义的标准接口可能成为传达条件和要求的简便方法，以使供应商成为组织生态系统的一部分。这样的界面描述可能包括数据交换规则，工具和流程，它们将在多厂商环境中创建通用语言。

在组织旨在确保快速有效的事件解决的情况下，他们通常会试图与合作伙伴和供应商达成紧密的合作协议，消除沟通，协作和决策制定方面的正式官僚障碍（有关更多信息，请参见供应商管理实践指南）。

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培养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ITIL Foundation：ITIL 4 Edition的4.3节。

8 致谢

AXELOS Ltd非常感谢为本指南的开发做出贡献的每一个人。这些实践指南融合了ITIL社区前所未有的热情和反馈。AXELOS特别要感谢以下人员。

作家

Barry Corless, Roman Jouravlev, Andrew Vermes.

审稿人

Akshay Anand, Sofi Fahlberg, Michael G. Hall, Steve Harrop, Piia Karvonen, Anton Lykov, Paula Määttänen, Christian F. Nissen, Mark O'Loughlin, Tatiana Orlova, Elina Pirjanti, Stuart Rance.