# 监控和事态管理

## 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

本文档为监控和事态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
- 监控和事态管理的流程和活动及其在服务价值链中的作用
- 监控和事态管理中涉及的组织和人员
- 支持监控和事态管理的信息和技术
- 适用于服务财务管理实践的适用于服务财务管理实践的注意事项

## 1.1ITIL®4 鉴证方案

从本文档中选择的内容可作为以下课程的一部分进行检查：

- ITIL专家：创建，交付和支持
- ITIL专家：指导计划和改进

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

监控和事态管理实践的目的是系统地观察服务和服务组件，并且记录和报告选择标识为事件的状态变化。该实践标识基础结构，服务，业务流程和信息安全事件并对其进行优先级排序，并对这些事件建立适当的响应，包括响应可能导致潜在故障或事件的条件。

**事态**

对服务或其他配置项（CI）的管理具有重要意义的任何状态的变更。

监控和事态管理用于管理整个生命周期中的事件，以了解和优化在组织及其服务上的影响。监控和事态管理包括对与所有基础架构级别以及与组织及其服务使用者之间的服务交互作用有关的事件的标识，分类或分析。监控和事态管理确保对这些事件做出适当及时的响应。

实践的监控部分专注于服务和配置项（CI），以检测潜在重要条件，跟踪和记录服务人员和CI的状态，并将此信息提供给相关各方。

实践的事态管理部分着重于那些由组织定义为事态的受监视状态变化，确定其重要性，并识别并启动对它们的正确响应。有关事件的信息也会被记录，存储并提供给相关方。

监控和事态管理数据和信息是许多实践的重要输入，包括：

- 事件管理
- 问题管理
- 信息安全管理
- 可用性管理
- 性能或绩效和容量管理
- 变更使能
- 风险管理
- 基础设施和平台管理
- 软件开发和管理
- 其他。

关键点在于监控是事态管理发生所必需的，但并非所有监控都在事态的检测中产生。阈值和其他准则确定哪些状态更改将被视为事件。同样，重要的是要注意，并非所有事件都具有相同的重要性或需要相同的响应。准则将定义事态的类别发生了什么。按照重要性增加的顺序，典型类别是信息，警告和异常事件。

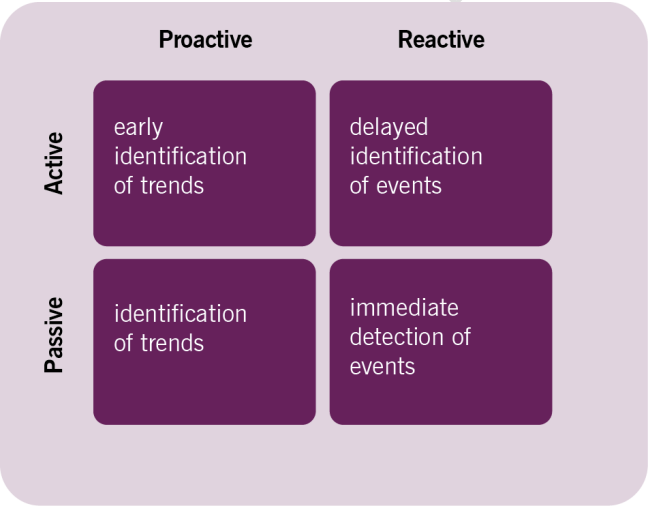
## 2.2 术语和概念

**监控**

重复观察系统，实践，流程，服务或其他实体以检测事件并确保已知当前的状况。

了解服务的状况和服务组件对于管理它们至关重要。有关服务运行状况和性能或绩效的信息使组织能够对已发生的服务造成影响的事件做出适当的响应（被动性监控），或者根据对过去事件的模式分析采取积极的行动，以防止将来发生不良事件（主动监控）。

监控通过多种不同的方式完成。CI可以通过轮询（即响应监控工具收集特定目标数据的请求）或通过在满足某些条件时自动通知监控工具来共享有关其自身的信息。监控工具对服务组件的质询代表计划实施检查改进，而CI向监控工具发送的通知的收集代表被动监控。




图片2.1 监控的类型

注意：当使用计划实施检查改进识别趋势时，它可能有助于识别早于被动监控的趋势（监控工具在CI自身发送信息之前先请求信息）。但是，当使用计划实施检查改进来检测事件时，它可能比被动监控迟一些：在计划实施检查改进中，信息是根据计划收集的，但是与被动监控一起，CI会在事态之后立即共享它。本注释的重要性取决于计划实施检查改进是连续的还是基于间隔的。重要的是要强调，从监控工具到服务和CI的请求之间的间隔时间越长，事件与其注册之间的潜在延迟就越长。

监控利用了正在观察的服务组件的本机监控功能。例如，有关操作系统（OS）的数据（例如磁盘空间，CPU负载，交换使用情况等）已经由OS公开，并指示底层物理资源的使用情况。同样，许多Web服务器，数据库服务器和其他软件都具有内置的监控功能，并将生成度量数据。所有这些数据都可以轻松发送到监控工具。

除了本机监控功能外，监控还采用了专门设计的监控系统。这些是用于监视Web和云应用程序，基础结构，网络，平台，应用程序和微服务的定制软件功能。对于某些服务组件，尤其是内部开发的应用程序，可能有必要向服务中添加自定义工具，例如，代码或接口，这些代码或接口收集并公开对于组织非常重要的度量数据。

尽管监控和事态管理传统上专注于服务的技术组件，但了解其他服务管理资源和活动（包括流程，人员和供应商）的状态也很有用。

**指标**

为管理和改进点监视或报告的度量或计算。

指标是监控和事态管理实践的原始数据的来源。监控系统收集，汇总和分析度量标准数据。指标涵盖多个层次，包括：

- 低级基础架构指标（主机，服务器，网络和其他）
- 应用程序指标（响应时间，错误速率，资源使用情况...）
- 服务级别指标，包括基础结构，连接性，基于应用程序和基于服务动作的指标（如果适用）
- 第三方服务绩效指标（基于公认的服务级别）
- 操作，流程和价值流性能或绩效指标。

**阈值**

触发预定义响应的指标的价值。

对阈值的响应可能有所不同，其中包括：

- 创建一个告警或其他通知
- 创建一个事件
- 先前记录的告警或通知的状况的变更
- 向各自的组件或服务启动被动式性能或绩效。

阈值是一种初始过滤可通过监控工具收集的大量监控数据的方法。阈值的值应谨慎定义，以防止生成过多的响应，并压倒资源，人力和机器的响应能力。处理度量数据的其他规则通常与阈值结合，例如事态相关规则和引擎。这些可以由组件供应商规定，由组织定义，或由机器学习支持。

监控和事态管理示例中的一些阈值示例可能是：

- 一小时内出现X个以上磁盘错误
- 在任何两个连续事件之间，CPU利用率达到或超过N％的次数超过N％的时间少于Z秒的三倍。

**告警**

通知已到达阈值，已更改某些内容或已发生失效。

警报由监控工具创建和控制，并由监控和事态管理实践管理。警报是监控系统的一个非常重要的方面。发出警报的系统必须具有几个特征，包括：

- 高度可靠
- 灵活，因此可以通过多种媒体通知操作员
- 能够生成详细且可行的通知消息。

对于监控和事态管理，“过度警报”是潜在的危险。出现这样一种情况，即生成的警报数量超出企业的处理能力，并且真正重要的警报丢失在“ 告警噪音”中。如今，通过人工智能操作（AIOps）和机器学习（ML）启用的警报的汇总，关联和过滤功能，为解决这种潜在的危险提供了解决方法。

服务和服务组件的状态更改在IT 环境中连续发生。如该实践中所述，通常可以通过IT服务，CI或监控工具创建的通知来识别它们。为了正确处理和响应数据的流，有必要对传入的信息进行过滤和分类。

状态变更的典型处理数据根据事件的影响将事件放入三个事态组之一，并定义三个相应的响应：信息，警告或异常。

- *识*别信息事件时，不需要性能或绩效。信息事件提供设备的状况或服务或确认任务的状态。信息事件的示例包括：用户登录，运维完成等。信息性事件表示正常的运维正在发生，并在设置的时间段内存储在日志文件中。组织可以选择在以后的日期分析信息事件，并且可以发现可能有益于服务的主动步骤。信息事件也可以在状况仪表板上发布，以供服务提供者或服务消费者的受众使用。
- *警*告事件使性能或绩效可以在经历任何负面的影响之前被采取。警告事件表示发生了异常但不是异常的运维。警告事态通知相应的团队或工具采取必要的措施，以防止发生异常。警告的示例包括：计划的备份未运行，或者资源的使用率在约定的例外阈值的10％之内。
- *异*常事件表示已达到服务或组件指标的关键阈值。标识为服务或组件性能或绩效的既定规范的违反可能尚未在业务运营上拥有影响。但是，异常事态也可能表示服务或组件正在经历失效，性能或绩效

降级或功能丧失。所有这些都是影响业务运营。无论哪种情况，异常事件都需要性能或绩效，因为它们表示正在发生常规运维的异常。异常事件的示例包括：PC扫描显示未授权软件的安装，服务器关闭，备份失败等。这是监控和事态管理实践启用事件检测的方式。

事态的分类将注意力集中在对于管理和服务交付真正重要的事件上。它可以确保对运行的事件进行适当的跟踪，评估和管理。

监控和事态管理启用事件检测，将其与信息事件和警告区分开。检测到的事件由事件管理实践处理。监控和事态管理还通过提供有关影响服务和服务组件的趋势和事件的信息来启用问题识别。此外，监控和事态管理启用错误控制来解决监控已知的错误，并报告服务和服务组件。已识别的问题和已知错误的错误控制由问题管理实践处理。

## 2.3 范围

监控和事态管理实践的范围涵盖了需求的需求可以控制并可以自动化的所有方面。这包括：

- 识别和优化监控的范围
- 实施和维护连续监控
- 建立和维护事态的标识，分类和处理规则
- 实施流程和自动化工具以操作已定义的事态管理规则
- 根据议定和实施的规则以及流程对事件进行持续处理
- 以商定的形式向有关利益相关者提供有关受监视服务和资源的当前和历史状态的信息。

尽管活动和责任领域仍与XTC5011密切相关，但它并不包含在其中。表2.1中列出了它们，以及对可以找到它们的实践的引用。重要的是要记住，ITIL实践只是价值流的背景中使用的工具的集合，应根据情况进行必要的组合。

**表2.1其他实践指南中描述的与监控和事态管理相关的活动**

| 实现价值 | 实践指南 |
| --- | --- |
| 管理事件 | 事件管理 |
| 调查事件和趋势的原因 | 问题管理 |
| 管理响应事件的更改 | 变更使能 |
| 与用户沟通 | 服务台 |
| 基于监控数据的支持决策 | 度量和报告 |
| 设置服务质量和性能或绩效的目标和阈值 | 服务级别管理可用性管理<br>性能或绩效和容量管理<br>信息安全管理连续性管理 |
| 设置基础结构和应用程序组件的阈值 | 基础设施和平台管理<br>软件开发和管理 |
| 设定第三方服务的目标和门槛 | 供应商管理 |

## 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。

监控和事态管理实践包含以下PSF：

- 建立和维护描述各种事件和检测它们所需的监控功能的方法/模型
- 确保及时，相关且足够的监控数据提供给相关的利益相关者
- 确保发现，解释事件，并在需要时尽快采取措施。

### 2.4.1 建立和维护描述各种事件和检测它们所需的监控功能的方法/模型

在大多数情况下，现代技术为测量和监视服务以及服务组件运维的各个方面提供了机会，但是从业人员应认真管理监控的范围以及度量的频率和数量。现代监控和事态管理实践的主要挑战不是缺少数据，而是监控必须处理的数据的体积。监控和事态管理实践的重点应该是获取有意义的信息，以支持服务的操作以及改进点，决策和价值的创建。建立或改进监控和事态管理实践时，应考虑以下方面。

- 识别和优先处理受监视的服务和服务组件

  实践的关键实现价值关键在于确定和优先监视哪些实体，这有助于检测状态更改（或缺少所需的状态更改），这些更改对于CI的服务的管理最重要。确定要监视的服务，系统，CI和其他服务组件将基于组织的业务目标。它还需要对组织的服务设计架构有透彻的了解。

  监控和事态管理的从业者将需要了解服务依赖映射：哪些顶级业务功能映射到哪些产品和服务支持那些功能，然后哪些产品和服务映射到支持该产品和服务的基础IT基础设施。通过完整地了解交付服务涉及哪些实体，监控和事态管理的从业人员将能够正确识别并确定需要监控的关键实体的优先级。

  这里，还应评估服务组件的“可监视性”，并定义有效的准则集。选择的准则应该具有足够的揭示性，并为诊断和决策提供基础。

- 在监控的信息性，粒度和频率之间找到平衡

  建立和维护服务的监控可以视为对资源（监控工具，数据存储，工时等）的投资，并且捕获的数据越多，预期的回报就越少。这是因为监视的准则数量和探测频率越多，用于过滤，分类和分析数据的时间和精力就越多。自动化和基于机器学习的解决方案可以帮助释放人员和数据分析数据的结果，但从业人员应始终致力于使监控效率最高。

- 数据的收集，存储，过滤和数据相关性的维护功能。监控和事态管理实践严重依赖服务管理的信息和技术尺寸。没有观察到服务和服务组件的本机监控功能，并且没有使用IT 监控工具（通用的通用商业工具以及定制工具），几乎不可能检测到对CI或服务具有重要意义的状态变化。
  服务元素通过轮询（即响应监控工具的询问来收集特定的目标数据），或者通过在满足某些条件时自动通知监控工具，来传达有关自身的信息。该通信取决于监控工具的可用性和传输事态数据的网络。
  应该特别注意执行分类的工具，数据的过滤和关联以及用于事态响应的自动化工具。

根据组织的业务和使命目标，确定要监视的服务，系统，CI和其他服务组件。它还需要对组织的服务架构有透彻的了解。监控和事态管理的从业者将需要了解服务依赖映射：产品和服务如何映射到启用它们的基础IT基础设施。通过完整地了解交付服务涉及哪些实体，监控和事态管理的从业人员将能够正确识别并确定需要监控的关键实体的优先级。

服务架构的大量单个服务通常由组织集成的第三方产品和服务组成，以向客户和用户提供端到端服务。这些第三方产品和服务的内置监控功能是监控和事态管理实践的关键部分。监控和事态管理从业人员以及服务设计实践中的同行需要能够与他们的设备和服务供应商经常且良好地合作。这样，监控和事态管理和服务设计可以保护构成组织服务的必要货品和服务，并确保这些服务是可监视和可管理的。

为事件确定适当的控制性能或绩效取决于对检测到的状态变化的过滤和分类。信息和技术服务维度中发生的过滤和分类在很大程度上由组织的事态管理体系（EMS）自动完成，IT 监控工具将检测到的，收集的和传输的信息馈送到其中。但是，业务规则通过EMS对数据进行过滤和分类，并确定它们的重要性（确定数据代表信息，警告还是异常事态）已建立在服务管理和服务管理的人员维度中。监控工具和EMS配置的阈值，警报参数，准则都是组织优先级的生产以及熟练的领导和工作人员，这些工作旨在确保运行的生态系统的健康。

需要制定策略来处理不同类型的事件。对事件采取“一刀切”的做法是不合适的，而且浪费资源。不同类型的事件需要针对事态的类型量身定制的响应。应该为每个事态类建立一套通用的控制操作。当适当的自动响应，适当的告警和升级对人为干预，何时应启动事件，问题或变更或需要特殊处理时，将解决策略。例如，在安全违规的情况下，它可能具有运行的影响，但尚未影响服务

availability.策略在组织和人员维度中定义，并在信息和技术维度中实施。

为事件（例如信息性，警告和异常）使用适当的标准分类方案可以启用通用处理和升级流程。它还使事态通知仅发送给负责处理与事件有关的进一步动作或决定的人员。通常，在事件，问题或变更管理中实践。避免向未直接参与事件处理的个人发送通知是对资源的有效利用。为此，事态通知将确定需要响应事件的部门，团体或个人。随着添加新事件或人员职责变更，维护事态路由信息是一项不变的任务。

针对事件的标准分类方案将能够为每种事态类建立一套通用的动作。在价值流中，当对已识别的事件采用性能或绩效时，服务的运行的和服务级别目标将纳入考量。触发事件和问题通知的事件操作可以与事件和问题管理已建立的现有分类和优先级策略绑定。

第三方供应商可能会提供许多IT 监控工具和EMS本身，与监控和事态管理实践和供应商管理实践保持稳定的工作关系。

### 2.4.2 确保及时，相关且足够的监控数据提供给相关的利益相关者

监控和事态管理的报告方面使服务提供者的实际运行性能或绩效和行为相对于原始服务设计和与客户达成协议的服务级别协议（SLA）中的标准成为现实。监控和事态管理提供直接的观察结果，与预期结果或理想结果相反的实际经验证据。

收集具有准确性的数据和监控和事态管理实践中的完整性对于使用服务时交付高质量服务和高质量客户体验的工作至关重要。服务度量（有关服务的数据的集合）取决于监控和事态管理监控和报告。由于监控和事态管理专注于服务的效果和效率以及服务组件，因此对于持续改进的工作至关重要。

监控和事态管理确定了薄弱区域，因此可以采用补救性性能或绩效（如果有正当的商业案例），因此可以改进将来的服务质量。监控和事态管理还可以显示客户动作在哪里导致故障，并确定效率工作和/或培训可以在哪些地方得到改善。监控和事态管理还可以同时满足内部和外部供应商的需求，因为必须同时评估和管理其性能或绩效。

### 2.4.3 确保检测，解释事件，并在需要时尽快采取措施

仅仅为监控和事态管理定义规则还不够。需要实际的检测和事件处理程序才能使这些规则有价值。事态管理的效率和范围在很大程度上取决于服务架构和服务管理自动化级别。在数字化基础结构和现代应用程序中，内置了许多用于监控和事态管理的工具，并且实践的重点是事态处理规则的集成和调整。

与此相反，拥有许多不是为监控设计的遗留系统的组织必须将重点放在专用监控和事态管理工具和附加组件的实现上，或者甚至集中在手动监控和事态管理上。

技术机遇和局限性应告知监控和事态管理，范围，策略制造和每日活动。

不管组织的监控和事态管理功能有多有限，都应遵守持续改进，以确保实践符合组织的需求。

## 2.5 关键指标

ITIL实践是管理产品和服务的手段或工具。像任何工具的性能或绩效一样，只能在该工具的应用程序的背景中评估实践性能或绩效。但是，质量中的工具可能有所不同。这种差异定义了根据用途使用该工具的潜力或能力是有效的。

同样适用于实践：应在价值流的背景中评估其性能或绩效，但其潜力由其资源的设计和质量定义。有关指标，KPI和其他可帮助解决此问题的技术的进一步指南，请参见度量和报告实践指南。

监控和事态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，以评估监控和事态管理实践对那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。

表2.2 实践成功因素的示例指标

| 实践成功因素 | 指标指标 |
| --- | --- |
| 建立和维护描述各种事件和监控功能所需的方法/模型<br>发现他们 | ● 监控和事态管理方法的利益相关者的满意度<br>● 组织对方法的坚持<br>● 未遵循或发现不切实际的方法建议/要求的百分比 |
| 确保及时，相关且足够的监控数据提供给相关的利益相关者 | ● 监控和数据的利益相关者的满意度及其演示<br>● 监控数据的质量（根据商定的数据质量准则） |
| 确保检测，解释事件，并在需要时尽快采取措施<br>可能 | ● 事态的影响管理错误<br>● 事态通信“噪音”的编号和影响<br>● 影响由于不良的事态管理而无法防止或解决的事件和问题 |

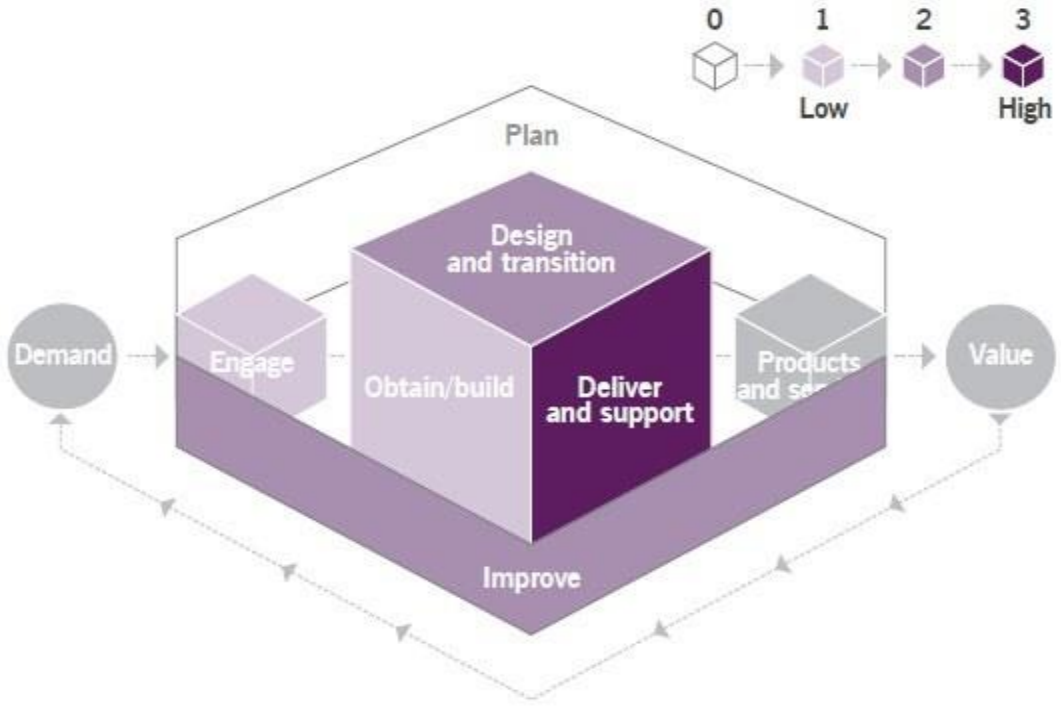
将指标正确汇总到复杂指标中将使它们更易于用于正在进行的价值流的管理和监控和事态管理实践的定期评估和持续改进。没有单一的最佳解决方案。度量标准将基于服务战略的整体和组织的优先级，以及实践所贡献的价值流的目标。

# 3 价值流和流程

## 3.1 价值流的贡献

像任何其他ITIL 管理实践一样，监控和事态管理实践也有助于多个价值流。请记住，没有价值流由单个实践组成。监控和事态管理实践与其他实践相结合，可以为消费者提供高质量的服务。

图片3.1中显示了监控和事态实践对服务价值链的贡献。




图片3.1 监控和事态管理实践对价值链活动的贡献的热图。

**监控和事态管理实践贡献的主要价值链活动是：**

- **交付和支持**
- **设计和转换**
- **改进。**

## 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。流程定义动作的顺序及其依赖性。

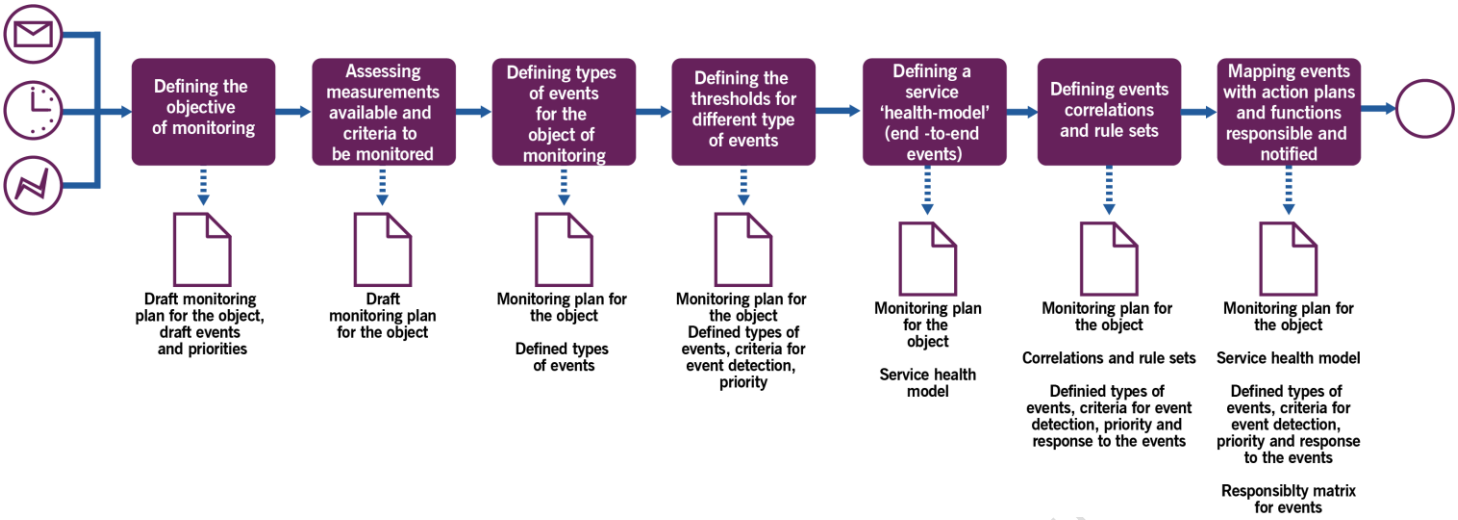
监控和事态管理实践活动形成三个流程：

- **监**控规划流程这是在监控中添加元素，定义元素的优先级，选择要监视的功能，为事态分类建立度量和阈值，映射事件与性能或绩效计划和负责的团队的流程。
- **事态处理流程**
- **监**控和事态管理评审该流程是针对主要事态事后反思计划或触发的评审流程，有关过滤和相关性分析的更新，服务“运行状况模型”，用于监控自动化和操作的改进。

### 3.2.1 监控规划

**表3.1 监控规划流程的输入活动和输出**

| 关键输入 | 活动 | 关键输出 |
| --- | --- | --- |
| 服务设计的服务健康状况准则<br>服务水平协议<br>可用性和容量和性能管理实践中的服务绩效阈值<br>知识文章服务目录<br>CI 数据 | 定义监控的目的<br>监视准则和准则的事件类型<br>监控的对象<br>定义不同事件类型的阈值<br>定义服务'运行状况模型'（端到端事件）<br>定义事件关联和规则集<br>使用性能或绩效计划和功能映射事件，并负责<br>已通知 | 监控计划用于对象服务健康状况模型<br>定义的事件类型，用于事态检测，优先级的准则以及对事件的响应<br>矩阵型的事件责任 |




图片3.2 监控规划流程的工作流程

**表3.2 监控的活动规划流程**

| 实现价值 | 描述 |
|---|---|
| 定义监控的目的 | 利用从服务设计阶段和服务验证和测试实践接收到的信息以及服务的开发涉及的实践（可用性，容量和性能管理实践）和服务级别管理实践，该团队确定了监控的关键目标。<br><br>讨论应从功效到功用需求（首先涵盖最明显的功能要求，例如，在应用程序的用户案例中）。另外，从键服务绩效开始，它的粒度应增加，然后移至更多详细信息和组件。<br><br>团队应列出监控降序优先级。 |
| 评估可用的测量并监视准则 | 然后，将监控优先级列表项映射或转换为可用测量或基于可用测量的综合测量。<br><br>应该探索添加度量。 |
| 定义监控对象的事件类型 | 团队对不同类型的事件进行定义和分类。类型可以是一般性的，例如信息性，警告性，异常性，也可以取决于功能，用户组及其优先级，再除以关键监控目标的组件或类型。 |

| | |
|---|---|
| 定义不同事件类型的阈值 | 团队与服务或组件开发团队一起定义事件类型的阈值。相同的组件指标可能是 |

| | |
|---|---|
| | 根据现有的SLA和针对服务或组件定义的可用性，容量和性能或绩效的要求，它基于服务进行了不同的处理。<br><br>另外，应该将处理吞吐量的事态纳入考量，因为尽管现代IT系统几乎可以检测到任何事态，但不应对任何事态进行操作。因此，从最初预防灾难到后来完善组件，通常都应将监控和事态管理开发为迭代。 |
| 定义服务'运行状况模型'（端到端事件） | 根据参与服务设计的团队的意见，构建了一个“健康模型”，它反映了服务中的关键事件及其之间的联系。一个服务可能有几种型号。<br><br>这样的模型使监控团队可以评估服务的用户体验。例如，可以为单个银行客户交易构建模型，并测量从移动应用程序中的请求（包括所有银行数据库系统到移动应用程序中完成交易的通知）花费的时间。<br><br>服务“健康模型”也可以实现为服务健康和性能或绩效的报告或仪表板，并由服务所有者，参与其他实践的团队和其他利益相关者临时使用。这样，有关服务的信息将被“拉”<br>利益干系人。 |
| 定义事态相关性和规则集 | 与参与服务设计的团队一起，定义了事态相关性和相应的规则集。<br><br>某些关联可能会使用第二个事态作为对第一个事态的检查，或者进一步过滤事态的范围。同样，定义的相关性可以帮助防止事件同时发生时可能产生的负面协同作用。<br><br>规则集由几个规则组成，这些规则定义了如何处理和评估特定事态的事态消息。例如，每次磁盘日志文件到达其容量时都可能生成警告事态，但是如果已生成四个以上的警告事件，则会生成异常事态。<br><br>规则本身通常嵌入监控和事态处理技术中。它们由布尔类型的算法组成，用于关联已生成的事件，以创建需要传达的其他事件。这些算法可以编入事态管理软件，通常称为关联<br>引擎。 |

| | |
|---|---|
| | 人工智能（AI）系统可用于定义用户，管理员，系统等的典型和非典型行为。这可能形成<br>其他检查以过滤事件。 |
| 使用负责并已通知的性能或绩效计划和功能来映射事件 | 对于每个事态或事件组，都定义了一个性能或绩效计划以最小化事态的负影响。基于性能或绩效计划，可以定义负责事态之后的动作的团队或职能。<br><br>性能或绩效计划还可以自动执行或半自动执行，包括对某些重要操作进行人工干预。<br><br>在此阶段创建的性能或绩效计划成为事态程序和自动化的基础。 |

## 3.2.2 事态规划

表3.3处理流程的事态的输入，活动和输出

| 关键输入 | 活动 | 关键输出 |
|---|---|---|
| • 来自监控，监控工具的对象的通知<br>• 监控计划 | • 事态检测<br>• 事态日志记录<br>• 事态过滤和相关性检查（可能是迭代的）<br>• 事态分类<br>• 事态响应选择<br>• 发送通知，响应规程执行 | • 事态记录<br>• 活动统计信息已更新<br>• 事态响应错误<br>• 重大事态事后反思启动<br>• 利益干系人通知<br>• 知识文章更新<br>• 记录的事件<br>• 更新的报告和仪表板 |

图片3.3处理流程的事态的工作流程

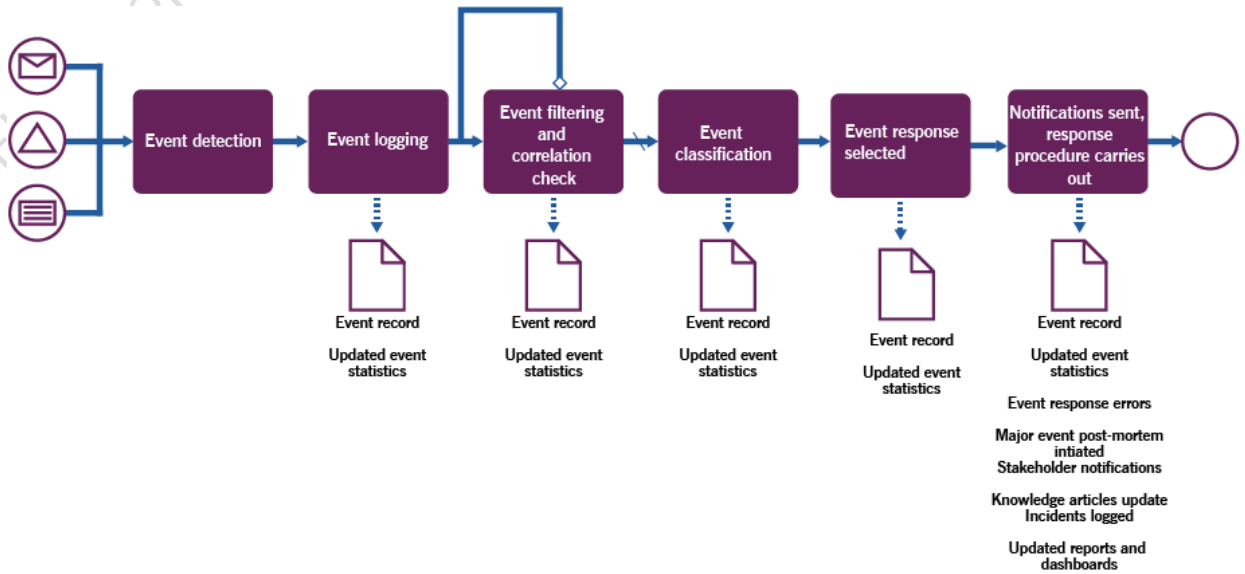


**表3.4处理流程的事态的活动**

| 实现价值 | 描述 |
| --- | --- |
| Event detection | 监控系统检测到的事态，或作为手动监控的结果。<br><br>并非所有事件都应被检测到，并且监控系统带宽应纳入考量。在现有资源中应仅检测到关键事件和可以采取行动的事件<br>约束。 |
| 事态日志记录 | 事态应该最好自动记录在监控系统中。 |
| 事态过滤和相关性检查（可能是迭代的） | 事态应该按照规则集进行处理，以过滤和查找相关性，以实现更好的分类。<br><br>该实现价值可能是迭代的。 |
| Event classification | 事态分为组或类型，如果需要选择适当的响应，则在组内进一步过滤特定的事态。 |
| 事态响应选择 | 应该为每个事态计划性能或绩效计划或响应规程<br>监控规划流程。根据规划中定义的规则，选择事态响应和通知的团队。 |
| 发送通知，响应规程执行 | 响应规程执行后，将通知负责操作或监督的团队（如果响应规程是全自动的）。 |

| 关键输入 | 活动 | 关键输出 |
| --- | --- | --- |
| ● 更新的知识文章<br>● 事态的主要记录<br>● 重大事件记录<br>● 改进点建议<br>● 事态记录和统计<br>● 服务所有者和利益相关者的信息请求 | ● 事后反思评审用于重大事件和事件<br>● 评审的过滤和相关分析<br>● 评审服务的“健康模式”<br>● 事态的评审响应程序和自动化<br>● 评审的工具可用于数据分析，相关性分析，AI和ML<br>● 评审收集的统计信息监控工具 | ● 更新了事态响应程序<br>● 改进点过滤和相关分析的建议<br>● 建议对自动化进行的更改<br>● 更新了监控准则和阈值<br>● 更新了过滤方法<br>● 更新了使用的工具和技术清单<br>● 提供了更新的报告和统计信息清单 |

### 3.2.3 监控和事态管理评审

**表3.6 监控和事态管理评审流程的活动**

| 实现价值 | 描述 |
| --- | --- |
| 事后反思评审用于重大事件和事件 | 重大事件发生的事实通常可能意味着未检测到某些异常服务或组件行为并对其采取了措施。因此，重大事件和事件为监控知识发现和改进提供了良好的基础。<br><br>应审查主要事态的性质，分析事态的相关性，分解为组件甚至CI水平，并应探索相应的指标，这些指标可能有助于检测导致重大事件的主要事态或失效。<br>应探索组件的其他或类似风险，并将已识别的事件添加到监控中。 |

| | |
|---|---|
| | 建议对监控进行更改以检测类似的内容<br>未来的事件。 |
| 评审的过滤和相关分析<br><br>评审服务的“健康模式” | 当监控检测到大量事件或应该检测不到事件时，应解决过滤和相关问题。有时可以考虑采取临时措施，例如放宽阈值或事件分组。否则，应进行详细分析和详尽的规则定义<br>进行，因此建议对监控进行更改。 |
| 事态的评审响应程序和自动化 | 事态响应结果中发生的事件和故障应进行检查并提出更改建议。<br>同样，此评审的目标应是提高事件检测和响应事件的自动化程度。应该建议附加的自动化。 |
| 评审的工具可用于数据分析，相关性分析，AI和ML | 内部和市场上可能会增加监控的效率的工具应进行审查。应在监控预算中提出试运行实现的试验。<br>另外，此评审应该讨论监控中使用的任何新技术或最佳实践，应该进行市场基准测试的开发，并提出对监控的改进。 |
| 监控工具收集的统计信息评审 | 应该审查统计信息，以提出对监控的改进，并监控服务。<br>服务生命周期涉及的所有团队均应审查检测到的服务趋势。 |

# 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。实践指南着重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以下模型的能力概况：

| 能力代码 | 描述 |
| --- | --- |
| L | 领导者活动和与此能力相关的技能包括决策<br>制作，授权，监督其他活动，激励措施和动机，以及评估结果。 |
| A | 管理员活动和与此功能相关的技能包括任务的分配和优先级，记录的保存，正在进行的报告以及基本的改进倡议。 |
| C | 协调员/沟通者活动以及与此能力相关的技能包括多方的协调，利益相关方之间的沟通以及认知销售活动的运行。 |
| M | 活动的方法和技术专家以及与该能力相关的技能包括设计和工作技术的实施，程序文档，有关流程的咨询，工作分析以及持续工作<br>改进点。 |
| T | 技术专家此能力专注于技术（IT）专业知识和基于专业知识的任务。 |