高新兴科技集团股份有限公司

受　　控

事件管理过程

文件编号：GSB/T 316.08

文件版本：A2

批　　准：刘伟辉

实施日期：2015-11-3

受控状态：受控

版本记录

版本	日期	修订页次	制/修订记录	制/修订者
A0	2013-12-18	/	新版制定	罗建明
A1	2014-10-22	9	“6.2 过程描述”有部分内容修订	罗建明
A2	2015-11-03	11	“7.2.4 重大事件沟通计划”部分内容有修订	李旻

目　　录

事件管理过程

1 目的

事件管理是为了减少或消除存在或可能存在于维护服务中的干扰因素给维护服务带来的影响，以确保用户可以尽快恢复自己的正常工作。因此，将事件记录下来并分类，再分配给适当的专业人员处理，同时监控事件的发展，并在事件得到解决之后将其关闭。

事件管理流程主要功能是尽快解决日常工作环境中出现的事件，保持维护服务的稳定性，其目的包括：

1) 在成本允许的范围内尽快恢复服务；
2) 快速响应服务请求(电话，邮件，ITSM 系统，即时通讯工具，现场)；
3) 跟踪事件处理的状态；
4) 确认事件的解决和用户满意度；
5) 进行事件控制；
6) 按规范记录事件；
7) 就事件的优先级、影响范围等进行分类；
8) 分析，诊断，必要时进行升级；
9) 监视并结束事件；
10) 进行定期服务回顾；
11) 提供一个日常服务接口。

2 范围

事件管理范围包括在服务工作中产生的操作咨询和故障处理，主要包括：

1) 服务请求和技术咨询：信息系统使用过程中，安装、部署、配置和使用等技术咨询。信息系统升级、扩容和改造等技术咨询活动。
2) 故障处理：对信息系统的软件和硬件故障进行处理。
3) 信息安全事件：由于网络、主机和操作人引发的有关信息安全事件。

3 术语和定义

事件是指在某一服务中不属于标准操作的并能导致或可能导致这个服务中断或服务质量下降的事件。

服务请求是用户想要获得有关的支持、提供、信息、建议或文档而提出请求，它并不属于维护基础构架方面的故障。

事件管理流程是负责解决维护服务的突发事件的运维流程。它的目的是尽快恢复被中断或受到影响的维护服务，所以它的特点往往是以解决表面现象为目的，而不在于查找根本原因。

术语	定义
维护服务	公司承诺的对客户提供的系统运行维护服务。
一线支持	服务台支持，主要包括服务热线，初级技术员和驻点技术服务工程师。
二线支持	维护维护支撑部非驻点工程师提供的软件和硬件技术支持，包括高级技术工程师。
三线支持	指供应商或生产厂家提供的技术支持。
重大事件	客户合同中规定的重大事件。

4 管理职责

4.1 过程负责人

事件管理负责人。

4.2 主要输入

输入	来源
服务热线、ITSM 系统、邮件、即时通讯工具（QQ、RTX）、现场	客户或维护人员

4.3 主要输出

输出	去向
客服热线电话记录	ITSM 系统中
ITSM 系统服务记录	ITSM 系统中
客户日常咨询问题汇总表	运维项目组

4.4 职责权限

事件管理负责人（运维项目经理）

主要具有以下职责：

1) 定义并维护事件管理流程文件及所需要的记录模板；
2) 管理事件管理流程的实施，包括一线、二线、三线的执行情况；
3) 确保事件管理流程目标的实现；
4) 识别事件管理过程中存在的问题并及时向部门经理提出；
5) 定期向部门经理汇报实施过程中存在的问题；定义并维护事件管理流程文件及所需要的记录模板；
6) 负责知识库的扩充、完善和修改。

一线支持（服务台客服员和驻点运维技术人员）

主要具有以下职责：

1) 收集有关事件解决方案的历史数据；
2) 事件的调查和诊断；
3) 根据解决方案把事件的影响降到最小，并确保快速恢复到正常服务水平；

4) 遇到事件无法解决，将事件提交给相关二线或三线支持，必要时进行事件升级，上报部门总监；
5) 与服务请求的提交者或其他相关用户进行直接的沟通、跟踪、通报问题的处理情况；
6) 将事件的解决步骤文档化，并录入后台；
7) 事件解决后，让用户进行确认事件已解决；
8) 结束事件，根据维护的实际情况更新相关信息。

二线支持（非驻点工程师）

主要具有以下职责：

1) 负责解决一线支持提交问题，把事件的影响降到最小；
2) 收集有关事件解决方案的历史数据；
3) 事件的调查和诊断；
4) 根据解决方案进行服务恢复；
5) 对利用“替代方案”解决的事件，在资源及时间允许时应找到事件根源；
6) 将事件的解决步骤文档化；
7) 跟三线支持之间的接口，如事件无法解决，将事件转发给相关三线技术支持；
8) 必要时向部门经理汇报并进行事件升级。

三线支持（外部产品供应商）

主要具有以下职责：

1) 与产品供应商有约定的服务协议，针对某个领域的服务的第三方承包商；
2) 在规定的时间内解决事件；
3) 对利用“替代方案”解决的事件，在资源及时间允许时应找到问题根源；
4) 在需要时及时利用其它资源(如：开发商，厂家)参与事件解决；
5) 将事件的解决步骤文档化；
6) 根据解决方案进行服务恢复；
7) 协助二线或一线完成事件分析和处理。

4.5 过程重要控制点

需要转二线支持、三线支持解决，由一线支持负责跟踪，直到确认事件关闭。

4.6 过程测量指标

通过对指标的分析，可以有效地对流程的运行情况进行监控和改进。事件管理流程 KPI 指标设置如下：

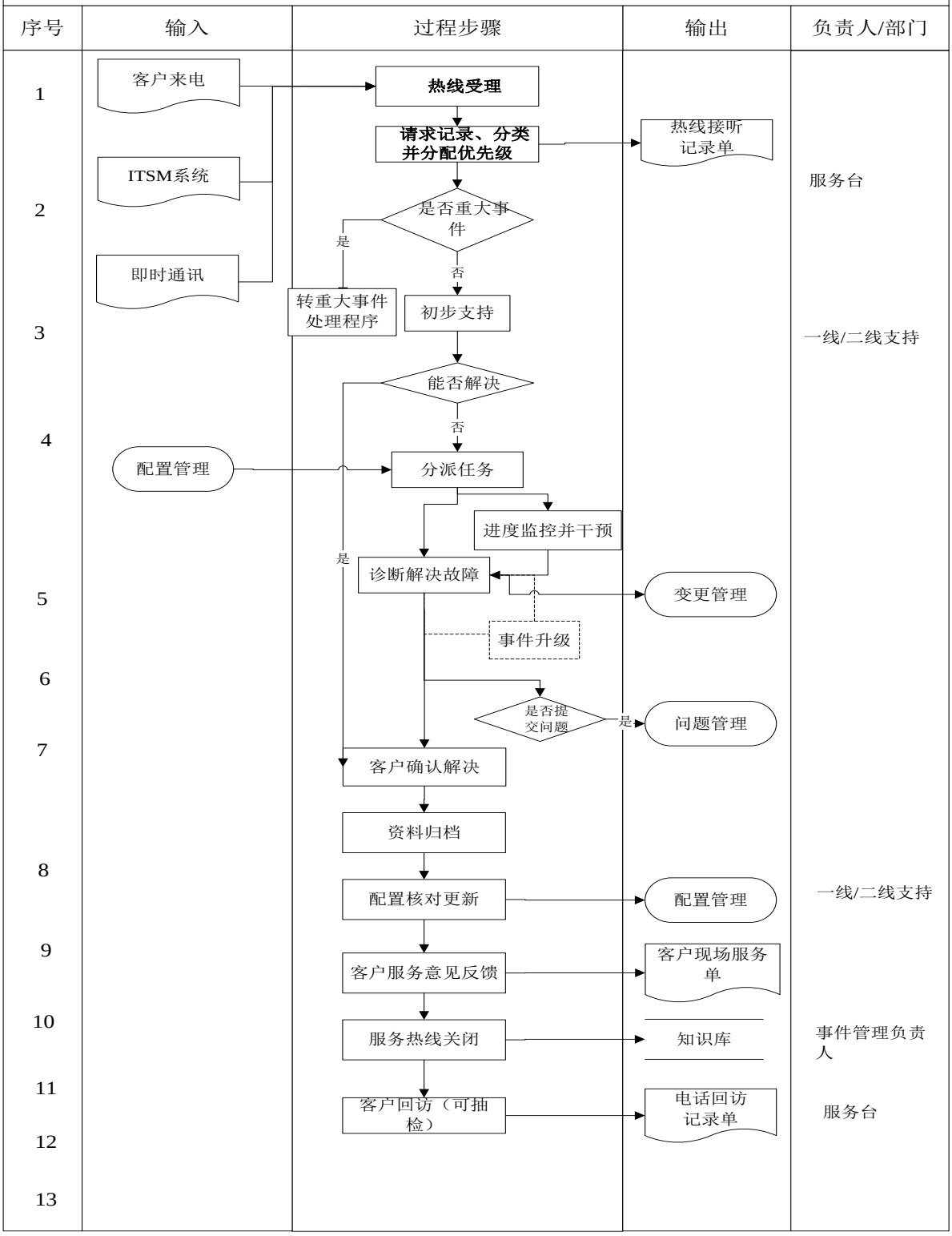
序号	衡量指标	指标说明
1	事件解决率	数量：在事件总数中过滤【事件状态】＝‘已关闭’ 比率：数量 / 事件总数 × 100 %
2	事件的平均解决时间	事件解决总时间/事件总数

事件流程负责人每季对事件处理的监控数据进行分析统计，形成服务报告。

5 工作流程

事件管理过程流程图如图 1 所示。

图1、事件管理流程一



6 管理过程策略和描述

6.1 过程策略

6.1.1 责任人策略

1) 用户通过电话，邮件，ITSM 系统，即时通讯工具，现场等方式向服务台报告事件，服务台当班人员接到事件报告和服务请求后，及时在维护 SM 系统内作好记录，服务台当班人员为此事件的负责人。
2) 服务台记录事件后，要分析事件是否在受理责任范围内。如果在受理范围内，根据事件单分类派给相关事件处理人员，并通知事件处理人，要求事件处理人员回复对分派的事件单是否接受。
3) 服务台当前值班人员负责向用户及时通报事件处理情况。
4) 事件解决后，服务台当前值班人员及时对申告人进行回访。

6.1.2 分类策略

由于用户提供的信息或许不完整或不正确，可能导致开始的分类与最终的分类有很大的差别。首先对事件按照基本事件类型进行分类，各类可以对应到相应的支持组，以便准确分配任务。

事件分类示例：

分类	说明
服务请求	如：状态查询、重置口令，业务咨询，信息咨询，工单处理等。
平台软件故障	平台软件出现问题，如错误提示、登击不了、联系不了在线设备等。
服务器 应急故障	机房服务器出现硬件故障，如系统停机、异常启动。
硬件故障	设备出现故障，如前端摄像头、交换机故障、防雷设备故障等。

事件状态：

编号	状态	描述
1	待处理	已在系统中记录，未派单给工程师。
2	已派单	已分配至工程师，工程师未处理。
3	处理中	工程师正在处理过程中，事件还未解决。
4	已解决	工程师已解决，服务台还未确认。
5	挂起	工程师正在处理，调用三线厂商支持或送外修，尚未完毕。
6	关闭	服务台确认，事件关闭。

6.1.3 优先级策略

给事件分配优先级，以保证支持组对事件必要的重视。分级应基于是事件的紧急程度和影响面。所有事件都应划分到不同的优先级中，其中划分为重要紧急的事件优先级为最高，根据事件的影响度和紧急度确定事件的优先级，事件优先级分为三级。

事件级别	级别定义			
	影响业务程度	影响业务范围	业务修复紧急程度	恢复时间要求（小时）

紧急（或重大）事件	系统在运行中出现瘫痪或服务中断，导致系统的基本功能不能实现或全面退化的故障。	100%视频监控业务受影响	重要（紧急）	2
严重事件	系统在运行中出现的故障具有瘫痪或服务中断的潜在危险，并可能导致系统的基本功能不能实现或全面退化。	部份视频监控业务受影响	紧急	5
一般事件	单一设备或普通的应用系统故障，导致小部分客户的服务受到影响；或某一应用系统实时性要求不高，故障造成的影响不大。	个别视频监控业务受影响	一般	8

事件分类与故障等级与技术支持合同相关，如有合同定义，则以合同定义为准。

6.1.4 目标解决时间策略和升级策略

为了更好的控制事件的解决，事件被分类分级，每类事件的解决都设定了目标时间。

升级策略的目的是确保不同优先级的事件分配到合适的资源来解决。为了达到这个目的，定义了升级策略的时间框架。当达到其时间界限时，如果事件还未解决，将触发升级机制。

事件升级时间表：

事件级别	**事件所处阶段**	**事件汇报人员范围**					
		项目经理（处理部门、服务台）		**部门总监（处理部门、服务台）**		**公司领导**	
		短信	**电话**	**短信**	**电话**	**短信**	**电话**
紧急（或重大）事件（2小时内解决问题）	事件发现10分钟内	√	√	√	√	√	√
	每30分钟或有新进展	√		√		√	
	事件解决后10分钟内	√		√	√	√	√
严重事件	故障发现	√	√	√			

（5 小时内解决问题）	20 分钟内						
	每 1 小时或有新进展	√		√			
	事件解决后 20 分钟内	√		√			
一般事件（8 小时内解决问题）	故障发现 30 分钟内	√					
	每 2 小时或有新进展	√	超 1 小时				
	事件解决后 30 分钟内	√					

6.1.5 裁剪策略

1) 项目经理或服务经理应和客户商定事件的分类、分级标准，事件的升级机制。
2) 项目经理或服务经理可根据项目环境裁剪本过程，报经过程管理组批准。

6.2 过程描述

6.2.1 热线受理

客户通过热线电话、邮件、即时通讯报告事件，服务台当班人员记录好相关信息，受理并进入事件处理流程。

服务台需要收集以下信息：

1) 来电客户的单位名称、联系人、电话号码等基本信息。
2) 影响业务的具体原因、故障现象以及所属优先级。

如果为重大事件，则需要上报给重大事件经理。

6.2.2 请求记录和分类

对于来自热线电话、邮件、即时通讯收集的信息，服务台记录《维护服务派工单》，通过电话方式申告的需要询问客户详细的事件描述，然后根据用户的描述判断事件的分类、优先级等信息。

如果事件是关于供应商的问题，根据合同协议，直接转三线支持。若事件比较重大且优先级为重要紧急，则需要报告项目经理和部门总监。

6.2.3 热线电话尝试解决

一线支持人员（服务台）受理事件后，首先根据用户所描述故障情况，参照《知识库》，对用户进行相应的指导解决。

一线支持人员（服务台）无法通过电话指导客户解决的事件，在征得客户同意的情况下，可以采用远程工具，登录客户计算机来操作解决。

6.2.4 分派任务

经一线支持人员（服务台）尝试解决无果或经判断不属于一线支持能力范围内的，提交二线支持解决。二线在技术上指导一线完成，或直接远程和现场服务。

技术研发团队：虚拟团队，负责研究解决运维中遇到的疑难问题，并分析其问题原因。

公司管理层：负责运维人员新增、调配及各种配套服务设备添加、调配的审批，并牵头解决重大的故障或者服务中产生的纠纷问题。

6.2.5 调查解决故障

现场服务人员（一线、二线、三线）在现场通过标准配置进行比对等方法对故障进行分析，查找出故障原因。

技术服务人员根据故障分析结果确定解决方案，并与客户沟通执行解决方案所需要的时间，确定解决方案的可行性。若发生的事件一时解决不了， 需要与客户约定解决时间。对于重大故障（故障等级为高或中）须做好数据备份。

若故障处理时涉及一般、重大、紧急的变更，转变更管理流程，参考《变更管理程序》。

事件解决后，故障现场负责人分析若属于影响重大或经常出现的问题，需要通过问题管理进行彻底解决的，转问题管理流程，参考《问题管理程序》。

6.2.6 客户确认

待事件处理完毕，需要与客户确认，若涉及上门服务，还需要客户在《维护服务派工单》签字确认。

6.2.7 资料归档

技术支持人员将《维护服务派工单》进行归档。

6.2.8 配置核对更新

当事件处理后配置项属性需要变更时，则由一线支持提交配置管理负责人进行配置项修改，修改设备台账中系统配置信息，参考《配置管理程序》。

6.2.9 服务关闭

当产生新的解决方案时，需要提交到知识库，对知识库进行相关的维护，该事件服务结束。

6.2.10 客户回访

服务台每月对事件处理结果对客户进行抽访，回访结果记录在《回访服务登记表》。

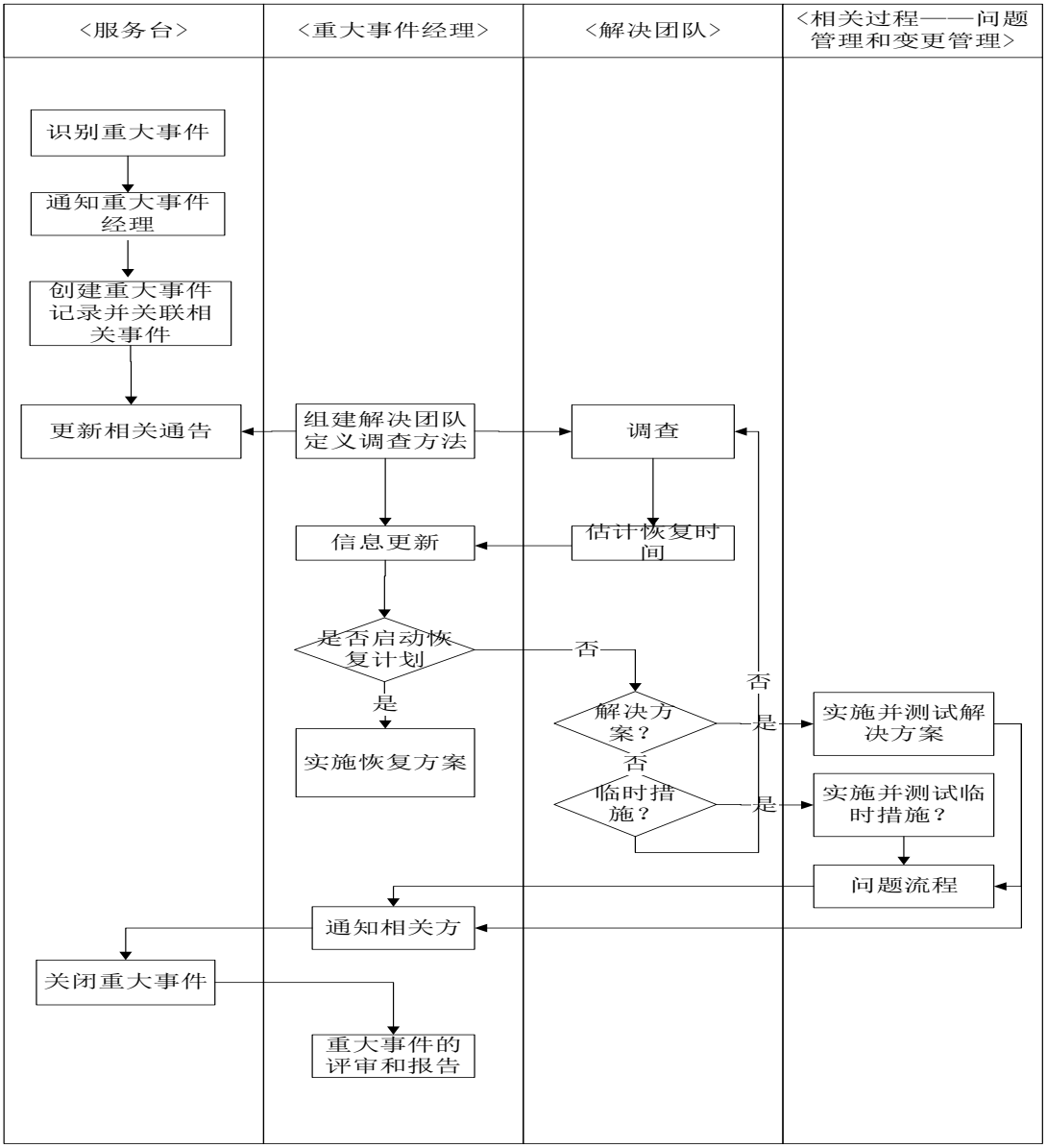
6.2.11 服务报告

运维项目经理按每个季度对事件进行总结并分类，并将报告发给部门主管再上报，必要时须提交客户。 事件报告内容包括（不限于）：

1) 本季度事件总数；
2) 本季度服务响应总数；
3) 解决事件总数；
4) 与历史报告比较的趋势分析和预测。

7 重大事件处理流程

7.1 流程图



7.2 流程描述

7.2.1 重大事件经理

重大事件经理负责在重大事件期间协调计划、资源和沟通。这是个临时性的职位，通常由技术副总担任。如果要昼夜不停地处理事件，则可能需要向单个事件分配多个重大事件经理。

扮演重大事件经理角色的职员需要满足下列条件：

1) 能够处理重大事件期间产生的压力。
2) 有权作出决定的高级经理。
3) 优秀的沟通者，能够与组织中的所有层次的技术维护职员、业务代表和客户交谈。
4) 深入了解公司（包括公司如何运作以及相关负责人）的公认人物。
5) 准备加班工作，经常是随叫随到。
6) 准备旅行并在需要时拜访客户现场，同样是随叫随到。

7.2.2 重大事件恢复小组

重大事件经理，应该收集到目前为止可用的所有信息，并确认当前状况并负责组建恢复小组。

调查和解决重大事件所涉及的技术团队称为“恢复小组”。该小组通常包含一个或多个技术人员，由同时经过技能培训和问题解决技术培训的资深职员组成。这个核心小组应该接受使用中的所有关键战略技术的培训，当时如果特定事件要求不同的技能，可以由其他支持人员提供补充。资深支持人员应该在临时分配的基础上在整个核心小组中轮流。

7.2.3 重大事件恢复计划

重大事件经理应该主持一次与恢复小组、已经参与处理事件的任何团队成员、受影响的经理和其他任何相关技术专家进行的初始计划会议。该会议的目标应该是同时就恢复计划和沟通计划达成一致。

恢复计划的目标是提供用于服务恢复的有计划和协调的方法。该计划由重大事件经理所有，并且应该对需要采取的操作、谁应该执行操作以及应该在何时完成操作等事项进行文档记录。应该在重大事件的整个生命周期中定期更新该计划，确保保留旧版本以用于审核目的。

恢复计划应该包含以下内容：

1) 截止目前已知的“问题”的陈述。
2) 事件的细分，详细描述组件、接口和可能的问题原因。
3) 关于如何检验或排除每个可能的直接原因的高级计划。
4) 根据可能性和确认的容易性权衡每个可能的原因，允许向每个可能的原因的调查赋予一个优先级。
5) 将在此阶段采取的调查或解决操作（基于所分配的优先级）的详细信息。
6) 关于谁将执行调查或解决操作的详细信息。

每个操作的执行时间表，以及下一次恢复团队复查会议的时间。

7.2.4 重大事件沟通计划

重大事件经理应该与包含运维管理中心经理、 维护技术中心经理、项目经理、受影响的业务的用户代表，和合作伙伴一起组建管理小组，定时复查进度。目的应该是讨论进度，并在需要时提供管理升级上报。在主持管理审查会议之后，应该同意并签发进度更新声明。

管理小组和恢复小组审查会议通常应该保持独立，以便每个小组集中于与他们的角色相关的问题。恢复小组应该讨论技术问题，然后为管理小组提供进度报告，后者然后可以集中于资源、上报和沟通问题。

在重大事件期间，沟通的处理本身经常变得非常困难。沟通计划的目标应该是在事件生命周期中提供所有沟通的协调。沟通计划应该由重大事件经理编制，并在每次管理小组审查会议时讨论和更新。该计划应该包括：

1) 谁需要定期更新。
2) 各方的详细联系信息需要更新。
3) 所需的不同类型的更新，取决于接受沟通的受众，可能需要不同的更新消息。
4) 高级管理更新。
5) 针对所有职员的更新。
6) 针对客户的更新。
7) 针对合作伙伴的更新。
8) 针对处理重大事件的职员的更新。
9) 新闻/媒体声明。
10) 针对紧急服务/机构的更新。
11) 每种类型的更新需要频度和下一次更新的到期时间。
12) 谁被授权同意每个不同的更新声明的发布。
13) 将传递每个更新的机制。
14) 下一次管理小组会议的时间。

一旦批准了沟通计划和恢复计划，则应该分配任何需要的附加资源。所有资源都应该能够访问恢复计划，以便他们能够看到截止目前已完成的操作和他们以及其他资源现在应该做的操作。

一旦重大事件过程已在进行中，计划已得到同意，资源已完成分配，就应该遵循调查、诊断、解决、恢复和终结的标准事件生命周期。重大事件的不同之处在于事件由重大事件经理所有并紧密协调，并在整个事件生命周期中定期审查和维护恢复和协调计划。

恢复小组应该以定期间隔支持审查会议以讨论进度、更新恢复计划并签发恢复小组进度报告。重大事件经理可以出席这其中某些审查会议，但是不一定要全部出席。审查会议之间的间隔视发生的活动量而定。例如，在调查的紧张阶段，该会议应该比职员只是等待确认解决操作成功时的后续阶段更加频繁。

还应该主持定期的管理小组会议以便向所有各方通气、讨论进度，并决定何时需要管理升级上报。重大事件经理应该出席所有管理小组进度会议。同样，审查会议之间的间隔应该视活动量而定。

在重大事件期间执行管理升级上报可能变得必要。随着事件变得更加关键，随着管理升级上报在合作伙伴和客户中的进行，沿管理链往上上报事件情况是必要的。这样可以避免诸如高级经理或主管首先从合作伙伴或客户组织的同行那里了解到事件的情况。

沟通计划应该随着管理升级上报或恢复小组成员变更而更新。重大事件经理负责在发布之前同意或获得所有沟通更新陈述的协议。

7.2.5 重大事件终结

随着重大事件的推进，重大事件经理应该确保定位、分配和协调任何附加资源要求。

有些重大事件可能使得调用组织的业务连续性和服务连续性计划变得必要。必须考虑到重大事件过程和服务连续性计划如何合作以及职责如何划分。在重大事件期间，重大事件经理决定何时以及是否应该调用服务连续性计划，以便恢复服务或保留恶意企图情况下的证据。通常，重大事件经理应该继续负责协调恢复操作、沟通和诸如收集证据和实施临时变通办法等活动。

重大事件过程应该继续伴随常规事件管理流程，直至重大事件终结。在事件的最后阶段，当已经采取解决操作时，解除恢复小组的部分任务也许是可能的，不过要了解到如果解决方案被证明不成功，他们将被重新召集。

在重大事件终结时，应该通知问题管理，因为执行重大事件后的审查是他们的职责。

8 相关文件

《问题管理程序》
《变更管理程序》
《配置管理程序》
《服务报告管理程序》

9 相关记录

《服务台记录表》
《知识库》（工作帮助文档）