



# 中华人民共和国国家标准

GB/T ××××—××××

## 信息技术服务 运行维护 第3部分：应急响应规范

Information technology service -  
Operation and maintenance-  
Part 3: Emergency Response

(送审稿)

××××-××-××发布

××××-××-××实施

中华人民共和国国家质量监督检验检疫总局  
中国国家标准化管理委员会

发布

目 次

目 次 ..... I

前 言 ..... 3

引 言 ..... 4

1 范围 ..... 5

2 规范性引用文件 ..... 5

3 术语和定义 ..... 5

4 应急响应过程概述 ..... 5

5 应急准备 ..... 6

5.1 应急响应方针与应急响应组织 ..... 6

5.1.1 应急响应方针 ..... 6

5.1.2 应急响应组织 ..... 6

5.2 风险评估与改进 ..... 6

5.2.1 风险识别与评估 ..... 6

5.2.2 风险控制 ..... 7

5.3 应急事件级别划分 ..... 7

5.4 预案制定 ..... 7

5.4.1 预案制定与评审 ..... 7

5.4.2 预案发布 ..... 7

5.5 培训与演练 ..... 8

5.5.1 培训 ..... 8

5.5.2 演练 ..... 8

6 监测与预警 ..... 8

6.1 日常监测与预警 ..... 8

6.1.1 范围 ..... 8

6.1.2 手段与工具 ..... 8

6.1.3 记录与报告 ..... 8

6.2 核实与评估 ..... 9

6.2.1 核实 ..... 9

6.2.2 事件级别评估 ..... 9

6.3 预案启动 ..... 9

6.3.1 预案启动 ..... 9

6.3.2 信息通报 ..... 9

6.3.3 监测与预警状态的调整 ..... 9

7 应急处置 ..... 9

7.1 应急调度 ..... 10

7.2 排查与诊断 ..... 10

7.2.1 手段工具 ..... 10

7.2.2 问题沟通与确认 ..... 10

7.3 处理与恢复.....	10
7.4 升级与信息通报.....	10
7.4.1 处置过程及结果的评审.....	10
7.4.2 升级.....	10
7.4.3 信息通报.....	11
7.5 持续服务与评价.....	11
7.6 事件关闭.....	11
7.6.1 申请.....	11
7.6.2 核实.....	11
7.6.3 关闭通报.....	11
8 总结改进.....	11
8.1 应急事件总结.....	11
8.1.1 对事件的总结.....	12
8.1.2 调查和取证.....	12
8.2 应急体系的保持.....	12
8.2.1 体系维护.....	12
8.2.2 体系审核.....	12
8.3 应急准备工作的改进.....	13
附录 A 规范的使用.....	14

## 前 言

本标准的附录 A 是资料性附录。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国信息技术标准化技术委员会归口。

本标准起草单位：

本标准主要起草人：

## 引 言

运行维护服务是信息技术服务中一个重要领域，为规范运行维护服务应急响应过程，提升应急响应能力，提前发现和解决问题，降低应急事件可能带来的不良影响，制定本标准。

本标准是信息技术服务运行维护服务相关系列标准之一。

本标准与 GB/T ××××. 1—××××、GB/T ××××. 2—××××、GB/T ××××. 4—××××、GB/T ××××. 5—××××等标准共同构成信息技术服务运行维护的相关配套标准。其中 GB/T ××××. 1—××××是通用要求，本标准、GB/T ××××. 2—××××、GB/T ××××. 4—××××、GB/T ××××. 5—××××等是在 GB/T ××××. 1—××××基础上的进一步细化和扩展。

本标准是根据现有信息技术运行维护服务的发展水平，提出和规定了应急响应的基本过程，本标准适用于指导国家安全、经济建设、社会管理、社会生活、生产经营等领域重要信息系统运行维护服务中应急响应的实施和管理。

# 信息技术 运行维护服务应急响应规范

## 1 范围

本标准是根据现有信息技术运行维护服务的发展水平，提出和规定了应急响应的基本过程。

本标准适用于指导国家安全、经济建设、社会管理、社会生活、生产经营等领域重要信息系统运行维护服务中应急响应体系的建设和管理。

## 2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分。然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

- ISO/IEC 20000-1:2005 信息技术—服务管理—第1部分：规范
- ISO/IEC 20000-2:2005 信息技术—服务管理—第2部分：实施指南
- ISO/IEC 27001:2005 信息技术 安全技术 信息安全管理体系要求
- GB/T ××××.1—×××× 信息技术运行维护服务通用要求
- GB/T ××××.2—×××× 信息技术运行维护服务交付规范
- GB/T ××××.4—×××× 信息技术数据中心运行维护服务规范

## 3 术语和定义

GB/T ××××.1—××××确立的以及下列术语和定义适用于本标准。

### 3.1

重点时段保障 important period protection  
需要提升服务等级，以确保某一时间段内重要活动或重点业务的开展所采取的措施和行为。

### 3.2

应急事件 emergency event  
导致或即将导致运行维护服务对象运行中断或运行质量降低或需要实施重点时段保障的事件。

### 3.3

应急响应 emergency response  
组织为预防、监控、处置和管理应急事件所采取的措施和行为。

## 4 应急响应过程概述

本标准规定了运行维护服务中应急响应过程的四个主要阶段：应急准备、监测与预警、应急处置、总结改进。如图1所示。

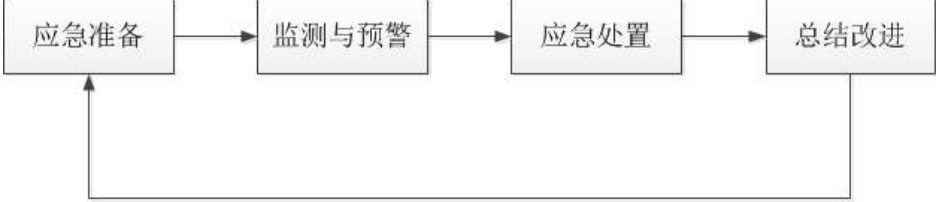


图1 运行维护服务应急响应过程

应急准备阶段的工作包括：组建合适的组织，以满足日常运行维护和应急响应的服务要求；系统性识别运行维护服务对象及运行维护活动中可能出现的风险，及时改进；对应急事

件进行级别划分，便于分级响应；制定预案，提供应对应急事件的操作性文件；开展培训和演练，以检验完善预案的需求符合程度，提高组织应急响应准备能力。

监测与预警阶段的工作包括：进行日常监测，保障运行维护服务的可用性和连续性，及时发现应急事件并有效预警；以规定的策略和程序启动预案，并保持对应急事件的跟踪。

应急处置阶段的工作包括：采取必要的应急调度手段，基于预案开展排查与诊断；对故障进行有效、快速的处理与恢复；通过实施有效评审，实现对应急处置的升级与通报；为应急事件的故障处置提供持续性服务保障，进行结果评价，完成事件的关闭。

总结改进阶段的工作包括：对应急事件发生原因、处理过程和结果进行总结分析，完善应急体系，实现对应急准备阶段工作的改进。

## 5 应急准备

### 5.1 应急响应方针与应急响应组织

#### 5.1.1 应急响应方针

组织应建立应急响应方针，明确应急响应的目标、原则、范围，并：

- a) 与相关利益方就应急响应的方针达成一致；
- b) 在计划时间范围内对应急响应方针进行评审；
- c) 在业务环境发生重大变化时对应急响应方针进行调整。

#### 5.1.2 应急响应组织

运行维护服务组织由相关利益方组成，如服务需求方、服务提供方、分包方、供应商等。

应急响应组织应在运行维护服务组织基础上建立，参与应急响应组织及组织内人员应确保属于提供运行维护服务的组织及人员，必要时也包括专家顾问及其他机构和人员。

应清楚规定运行维护服务及应急响应所有相关各方的角色及关系，并为关键角色准备备份人员。

应就运行维护服务及其应急响应服务的范围、要求、等级及沟通流程和方式与相关利益方达成一致，并形成记录。

运行维护过程中涉及组织及人员的变更应与相关方达成一致，并形成记录。

应建立对组织的重要评审过程。评审至少每年进行一次，以确保仍能继续满足运行维护服务和应急响应要求。

### 5.2 风险评估与改进

#### 5.2.1 风险识别与评估

组织应按照一个确定的方法和流程来实施风险评估，确保组织理解其在运行维护过程中的关键活动、所需资源、限制条件及组织面临的各种威胁。组织应理解当威胁演变为应急事件时所产生的影响和后果，以及业务中断所可能带来的损失。

应授权组织内或组织外的服务提供方进行风险识别，并将授权通知到所有相关方面。

被授权的服务提供方应结合具体的现状和要求，独立或与相关方面共同提出风险要素。

风险要素应从系统级的角度考虑，如运行维护对象、运行维护服务内容、组织及流程接口等。

应根据风险要素进行评估，评估可采用一种或多种方法相结合的方式，如定性评估、定量评估、基于知识的评估、基于模型的评估等。

分析评估后应形成报告，报告应包括：

- a) 与服务水平目标相适应的运行维护要求；
- b) 现状及趋势信息；
- c) 风险要素；
- d) 识别出的风险及建议的应对措施。

评估报告应在服务需求方授权的范围内进行评审和沟通，并达成一致。

确认后的评估报告应作为风险控制和预案制定的参考要素。

### 5.2.2 风险控制

对于识别出的各种风险,组织应该制定明确的控制策略。可供选择的风险控制策略包括:风险规避、风险转嫁、风险降低。

根据风险评估报告,组织应该形成改进方案以降低风险,可选择的方案包括:

- a) 降低风险转变为应急事件的可能性;
- b) 缩短应急事件的持续时间;
- c) 限制应急事件的影响范围。

### 5.3 应急事件级别划分

#### 5.3.1 参考要素

应急事件分级的主要参考要素为:信息系统的重要程度、紧急程度、系统损失和社会影响。

##### a) 重要程度

重要程度主要考虑信息系统所承载的业务对国家安全、经济建设、社会管理、社会生活、生产经营的重要性,以及业务对信息系统的依赖程度。

##### b) 紧急程度

紧急程度是指发现、响应应急事件,以及恢复系统正常运行的速度的要求。

##### c) 系统损失

系统损失是指由于应急事件导致系统业务中断,从而给事发组织和国家所造成的损失,其大小主要考虑恢复系统正常运行和消除应急事件负面影响所需付出的代价。

##### d) 社会影响

社会影响是指应急事件对社会所造成影响的范围和程度,其大小主要考虑国家安全、社会秩序、经济建设、企业组织和公众利益等方面的影响。

#### 5.3.2 级别划分

相关责任者应按照以上要素对可能发生的事件进行评估,确定应急事件的级别。

### 5.4 预案制定

#### 5.4.1 预案制定与评审

应根据风险评估和事件级别划分制定应急预案;预案可以分为总体预案和针对某个核心系统的专项预案及其附则;

预案中应该考虑到各种应急资源的调配和预置。应急资源主要包括人员、备品备件、资金、系统工具等。

预案的格式应该能够为应急响应人员进行系统恢复操作提供快速明确的指导。

预案应该明确、简洁,易于在紧急情况下执行,并尽量使用检查列表和详细规程。

应急响应预案的内容应包括:

- a) 应急响应预案的编制目的、依据和适用范围;
- b) 具体的组织体系结构及人员职责;
- c) 应急响应的监测和预警机制;
- d) 应急响应的启动;
- e) 应急响应的处置;
- f) 应急响应的保障措施;
- g) 应急预案的附则。

服务需求方应组织对预案进行评审,并达成一致。

#### 5.4.2 预案发布

经过评审确认的应急响应预案,应由责任者或被授权者负责预案的分发。



应确认应急响应参与工作的所有人员都接受预案。

应建立预案的版本控制。

## 5.5 培训与演练

### 5.5.1 培训

应制定应急响应培训计划，并组织相关人员参与。应急响应预案应作为培训的主要内容。

培训应使得相关组织及人员明确其在应急响应过程中的责任范围、接口关系，明确应急处置的操作规范和操作流程。

培训至少每年举办一次。

### 5.5.2 演练

为了检验预案的有效性，同时使相关人员了解运行维护预案的目标和流程，熟悉应急响应的操作规程，应按以下要求，组织应急响应的演练：

- a) 预先制定演练计划、演练脚本；
- b) 演练的整个过程应有详细的记录，并形成报告；
- c) 演练不能对业务运行造成负面影响；
- d) 按照与服务需求方的约定周期，进行有服务需求方（或被委托的第三方机构）参与的完整演练。

必要时，组织可根据演练的效果，对预案进行完善。

## 6 监测与预警

### 6.1 日常监测与预警

#### 6.1.1 范围

a) 应该对运行维护服务对象的运行情况进行监测与预警，以跟踪和判别以下对象的容量、可用性和连续性：

- 1) 应用系统；
- 2) 支撑应用系统运行的系统软件、工具软件；
- 3) 网络及网络设备；
- 4) 安全设备；
- 5) 主机、存储、外设、视频会议、桌面等设备；
- 6) 电力、空调、消防等基础环境。

b) 应该对业务数据进行监测与预警，以跟踪和判别业务数据是否超出了预警条件。

#### 6.1.2 手段与工具

服务提供方应结合运行维护服务级别协议和应急响应预案，开展日常监测与预警活动，包括：

- a) 设立服务台并保持运营；
- b) 确定监测项、监测时间间隔与阈值；
- c) 确定活动中的人员、角色和职责；

服务提供方可以采用运行维护工具与人工相结合的方式开展日常监测与预警活动。

#### 6.1.3 记录与报告

应建立监测、预警的信息登记和报告制度。

服务提供方应对日常监测的结果进行记录，并按照约定的形式和时间间隔上报相关责任者。

服务提供方发现应急事件时，应提交单独的报告，报告内容应包括：

- a) 故障或预警发生及发现的时间和地点；
- b) 影响的范围；

- c) 现象取证;
- d) 原因初步分析;
- e) 报告人。

报告应第一时间提交给相关责任者。报告方式包括电话、邮件、短信或书面报告等，并确认相关责任者收到报告。

应采取必要措施，开展应急事件的先期处置，以提高应急响应效率，避免次生、衍生事件的发生。

根据预案授权，由责任者或报告人作为应急负责人，统筹开展后续的核实与评估、预案启动、应急调度、排查与诊断、处理与恢复等工作。

应该对应急事件保持持续性跟踪。

## 6.2 核实与评估

### 6.2.1 核实

接到报告的责任者应对报告内容进行逐项核实，以判别应急事件是否属实。

核实确认后的应急事件报告，应作为事件级别评估的参考要素。

重点时段保障需求，也应作为事件级别评估的参考要素。

### 6.2.2 事件级别评估

责任者应参见应急准备活动中的事件级别划分，初步确定应急事件所对应的事件级别。

应将事件级别应置于动态调整控制中。

## 6.3 预案启动

### 6.3.1 预案启动

应建立、审议预案启动的策略和程序，以控制预案启动的授权和实施。

应就预案启动可能造成的影响进行评估。应在相关方之间就启动何种类型预案达成一致。过程应包括一旦事件升级，与之相对应的预案调整的方式。

可根据先期处置要求进行预案的自动启动，或由责任者或被授权者启动预案。

应记录预案启动的过程和结果。

重点时段保障应启动的预案可参考同级别预案确定。

### 6.3.2 信息通报

预案启动的责任者或被授权者应向服务提供方和其他相关方通报信息，内容应包括：

- a) 预案启动的原因;
- b) 事件级别;
- c) 事件对应的预案;
- d) 要求采取的技术应对或处置的目标;
- e) 实现目标所应采取的保障措施，如人员、物资、环境、资金等;
- f) 对应急处置过程及结果的报告要求，如报告程序、报告内容、报告频率等;
- g) 信息通报的范围和接收者。

信息通报的方式如电话、邮件、传真、书面文件等。

通报信息应作为调整监测与预警状态及后续活动的参考要素，后续活动包括应急处置、总结改进等。

所有相关方应对收到的通报信息进行确认和反馈。

### 6.3.3 监测与预警状态的调整

服务提供方应根据调整后的状态开展监测与预警活动，并按一致约定的程序和监测范围、监测频率提供报告。

监测与预警状态的调整应通知各相关方。

## 7 应急处置

### 7.1 应急调度

按照预案，开展统一的应急调度，包括物资、人员、经费等。

应急调度中还应注意：

- a) 尽快获取现场信息
- b) 迅速组织必要人员进行勘察、分析；
- c) 及时下达调度命令并保持跟踪；
- d) 保护可追查的相关线索。

### 7.2 排查与诊断

#### 7.2.1 手段工具

在排查与诊断中，应建立多渠道的应急处置支持模式，如：建立由服务商、供应商、生产制造商构成的应急处置支持模式。

故障排查与诊断的流程应包含以下内容：

- a) 应急处置责任者调配处置人员进行现场故障排查；
- b) 现场处置人员进行故障排查和诊断，必要时可寻求外协人员以现场或远程方式进行支持，在此过程中可借助各类排查诊断分析工具，如：应用软件、电子分析工具、故障排查知识库等；
- c) 现场处置人员应随时向处置责任者汇报故障排查情况、诊断信息、故障定位结果等；
- d) 将排查与诊断的过程与结果信息进行整理与归档；

#### 7.2.2 问题沟通与确认

在实施应急处置过程中，各级责任者应及时与相关利益方进行沟通，沟通的内容主要包括应急处置故障点、造成故障的原因、排查诊断等。

应及时完成对沟通信息及对应组织人员的核实与确认，同时对确认信息完成归档、上报、审批等事项。

应将问题沟通结果与确认信息告知相关利益方。

### 7.3 处理与恢复

应基于预案和知识库进行故障的处理与恢复，处理与恢复的原则包括：

- a) 应在满足相应服务级别协议要求的前提下，尽快恢复服务；
- b) 采用的方法、手段不应造成新的事件发生。

必要时可启用备品备件、灾备系统等。

应该对过程及结果信息进行记录，并及时告知相关方面及人员。

责任者应组织对处理与恢复的结果进行初步确认。

### 7.4 升级与信息通报

#### 7.4.1 处置过程及结果的评审

故障处置责任者应组织相关人员对故障处置过程及结果情况进行评审。

在评审中，应参考服务级别协议中对事件处置内容情况的设定，同时结合应急故障处置的现场情况进行分析和比较。

当应急故障现场处置的情况超过原应急预案中的事件处置级别要求时，应作为应急事件升级的参考要素。

#### 7.4.2 升级

应建立、审议应急事件升级的策略和程序，以控制应急事件升级的授权和实施。

应就事件应急事件升级可能造成的影响进行评估。应在应急处置涉及组织单位之间就确认事件升级达成一致。

升级过程应包含预案调整、人员调整、资金调整以及相关设施调整。

应急事件升级的实施授权应由明确的责任者或被授权者启动。

应对应急事件升级的过程和结果信息进行整理与归档。

#### 7.4.3 信息通报

应急事件升级的责任者或被授权者应向服务提供方和其他相关方通报信息，内容应包括：

- a) 事件升级的原因；
- b) 事件升级后的级别；
- c) 事件升级后与之对应的预案；
- d) 根据升级事件处置的要求和目标，确定所需的技术应对措施；
- e) 实现目标所应采取的保障措施，如：人员、物资、环境、资金等；
- f) 对升级事件处置过程及结果的报告要求，如：报告程序、报告对象、报告内容、报告频率等；
- g) 信息通报的范围和涉及接受者。

信息通报的方式如电话、邮件、传真、书面文件等形式。

通报信息应作为应急事件故障处置恢复的参考要素。

#### 7.5 持续服务与评价

在完成故障处置后，应组织运行维护人员提供持续性服务。

应对持续性服务的效果进行评价。

故障处置责任者应对已完成的故障处置和持续性服务阶段的运行状态，做出自评报告。

在相关方之间就持续性服务与评价报告达成一致的前提下，由明确的责任者或被授权者提出应急事件关闭需求。

持续服务的评价结果，应作为应急事件关闭的参考要素。

#### 7.6 事件关闭

##### 7.6.1 申请

应建立、审议事件关闭的策略和程序，以控制事件关闭的授权和实施。

应该对应急事件处置的过程文档和各评审/评价报告进行整理。

应由明确的责任者或被授权者提出事件关闭申请，并提交相关文档资料。

应急事件关闭申请和文档资料，应作为事件关闭核实的参考要素。

##### 7.6.2 核实

接到事件关闭申请的责任者应逐项核实报告内容，以判别应急事件处置过程和结果信息是否属实。

核实后的应急事件关闭申请报告，应作为事件关闭通报的参考要素。

##### 7.6.3 关闭通报

应建立、审议应急事件关闭通报制度。

应急事件关闭的责任者或被授权者应向相关利益方通报信息，内容应包括：

- a) 应急事件的级别；
- b) 事件对应的预案信息；
- c) 应急事件处置的过程情况；
- d) 事件的调整升级情况；
- e) 持续性服务状况信息；
- f) 事件处置评价信息；
- g) 事件关闭申请的处理意见；
- h) 关闭通报的范围和涉及接受者。

#### 8 总结改进

##### 8.1 应急事件总结

### 8.1.1 对事件的总结

在事件关闭之后，应组织相关人员对本次事件的原因、处理过程和结果进行分析，总结经验教训，并采取必要的后续措施。事件总结报告应该包含：

- a) 事件发生的原因分析；
- b) 应急事件的处理过程和结果；
- c) 评估应急事件造成的影响；
- d) 降低事件发生频率、减轻损害和避免再次发生的方法。

应根据事件级别、影响范围等因素，向相关方提交事件总结报告。

### 8.1.2 调查和取证

当一个事件涉及到责任认定、赔偿或诉讼时，应收集、保留和呈递证据。证据可能用于：

- a) 内部问题分析；
- b) 用作有关可能违反合同或规章要求的法律取证；
- c) 与供应商或其他组织谈判赔偿事宜。

## 8.2 应急体系的保持

为保证应急体系的有效性和时效性，需要对应急体系进行不定期及定期的维护和审核，以确保组织具有足够的应急响应能力。

体系维护主要是指当组织战略、业务流程、客户要求等发生重大变化的时候，对现有的应急体系，尤其是风险评估和应急预案进行修改。体系维护应该是不定期进行的，是由事件驱动的。

体系审核主要是指对组织当前的应急响应能力和管理模式进行评审，以确保它们符合预定的标准和要求，同时明确组织在应急响应方面的主要不足和改进方向。体系审核应该是定期进行的，组织应该至少一年进行一次体系审核。

### 8.2.1 体系维护

组织应该制定一个明确的应急体系维护计划。此维护计划应该确保任何影响到组织应急管理的重大变更都能被识别出来，同时采取必要的措施对这些变更进行分析，并对应急管理体系做出相应调整，这种调整可能涉及应急管理的方针政策、流程、应急预案和资源配置。

体系维护流程的结果应该包括：

- a) 关于应急体系维护活动的文档记录；
- b) 确保应急响应的相关人员都已经明确应急体系的调整内容，并接受必要的培训；
- c) 当需要对风险评估、组织架构、人员配备进行调整时，保留必要的文档记录。

### 8.2.2 体系审核

相关责任者应该按照预定的时间间隔对应急管理体系进行审核，以确保体系具有持续的适用性和有效性。体系审核应该包括评估体系不足和改进建议。体系审核的结果应该正式存档并通知给相关责任者。

a) 体系审核时应考虑的要素包括：

- 1) 相关利益方的要求和反馈；
- 2) 组织所采纳的用于支持应急响应的各种技术、产品和流程；
- 3) 风险评估的结果及可接受的风险水平；
- 4) 应急预案的测试结果及实际执行效果；
- 5) 上次体系评审的后续跟踪活动；
- 6) 可能影响应急体系的各种业务变更；
- 7) 近期在处置应急事件过程中的总结经验和教训；
- 8) 培训的结果和反馈。

b) 体系审核的输出结果应该包括：

- 1) 应急体系的改进目标;
- 2) 如何改进应急体系的有效性和效率;
- 3) 所需的各种资源, 包括人员、软硬件、资金等。

### 8.3 应急准备工作的改进

应急事件总结、体系维护和体系审核的结果应该作为应急准备阶段各项工作的改进要素。组织应根据应急事件总结报告中给出的建议项和体系评审结果来调整应急准备和风险控制策略。

附录 A 规范的使用

运行维护服务应急响应过程包括应急准备、监测与预警、应急处置和总结改进四个主要阶段，每个阶段中包括若干重点任务，这些任务覆盖了日常工作、故障响应和重点时段保障等不同类型的活动。下表描述了不同类型活动与重点任务的基本对应关系。

表 1：日常工作、故障响应、重点时段保障与任务的对应关系表

主要阶段	重点任务	日常工作	故障响应	重点时段保障
应急准备	运行维护组织建立	√		
	风险评估与改进	√		
	事件级别划分	√		
	预案制定	√		
	培训与演练	√		
监测与预警	日常监测与预警	√	√	
	核实与评估		√	√
	预案启动		√	√
应急处置	应急调度		√	√
	排查与诊断		√	
	处理与恢复		√	
	升级与信息通报		√	√
	持续服务与评价		√	√
	事件关闭		√	√
总结改进	事件总结		√	√
	应急准备工作的改进		√	√
	应急管理体系的保持	√	√	√