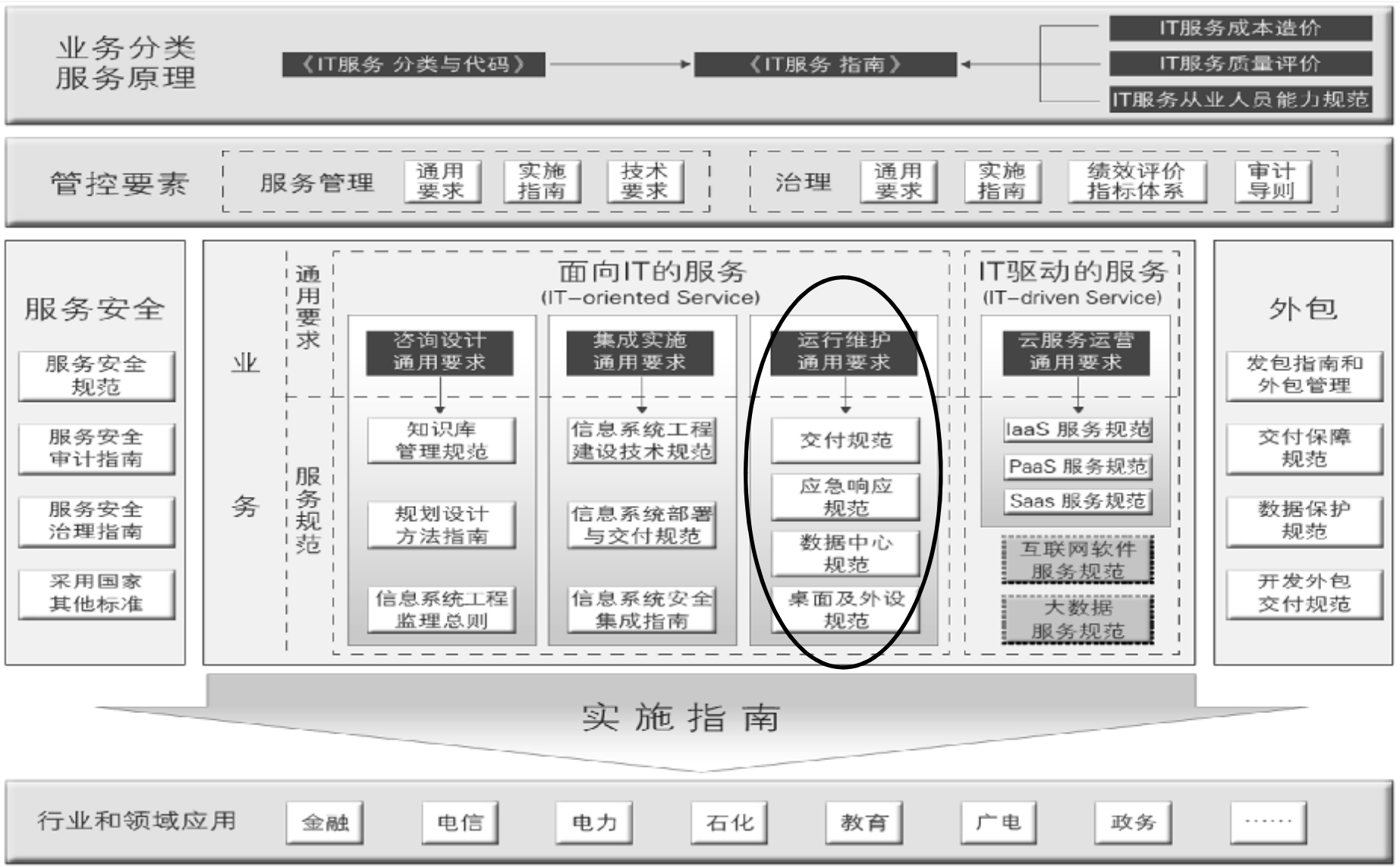
中国ITSS论坛

本讲堂授课录音： http://www.itilxf.com/thread-53290-1-1.html

国家信息技术服务标准（ITSS）
运行维护-应急响应规范

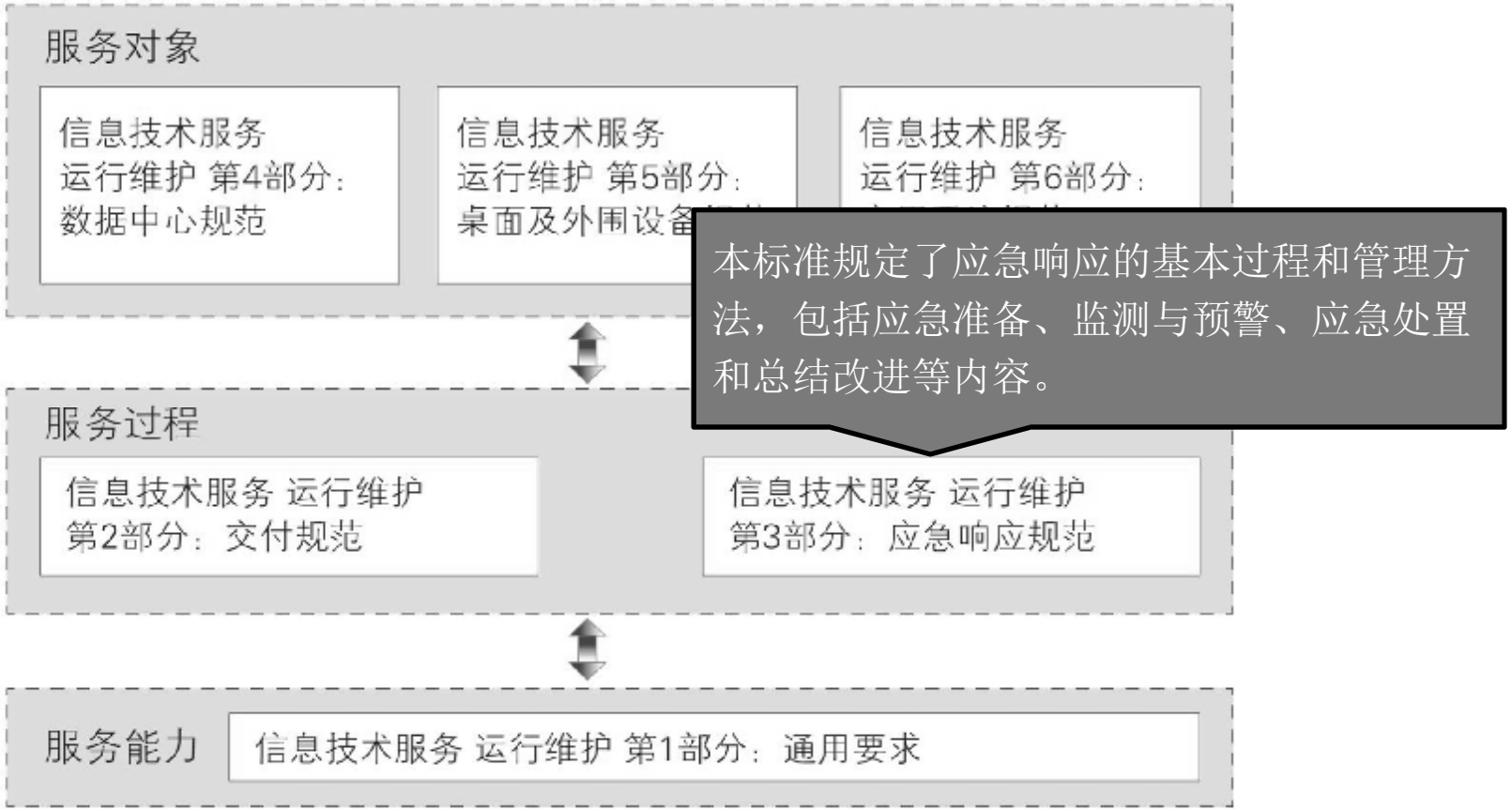
讲师：长河

ITSS体系框架


业务分类
服务原理
《IT服务 分类与代码》
《IT服务 指南》
IT服务成本造价
IT服务质量评价
IT服务从业人员能力规范
管控要素
服务管理
通用要求
实施指南
技术要求
治理
通用要求
实施指南
绩效评价指标体系
审计导则
服务安全
服务安全规范
服务安全审计指南
服务安全治理指南
采用国家其他标准
业务
通用要求
服务规范
面向IT的服务
(IT-oriented Service)
咨询设计通用要求
集成实施通用要求
运行维护通用要求
知识库管理规范
规划设计方法指南
信息系统工程监理总则
信息系统工程建设技术规范
信息系统部署与交付规范
信息系统安全集成指南
交付规范
应急响应规范
数据中心规范
桌面及外设规范
IT驱动的服务
(IT-driven Service)
云服务运营通用要求
IaaS 服务规范
PaaS 服务规范
Saas 服务规范
互联网软件服务规范
大数据服务规范
外包
发包指南和外包管理
交付保障规范
数据保护规范
开发外包交付规范
实施指南
行业和领域应用
金融
电信
电力
石化
教育
广电
政务
……

运维标准体系之间的关系

- **运行维护是信息系统全生命周期中的重要阶段，对系统主要提供维护和技术支持以及其它相关的支持和服务。运行维护服务的主要内容包括基础设施、硬件平台、基础软件、应用软件等IT基础设施，以及依赖于IT基础设施的数据中心、业务应用等信息系统**



标准术语

- **重点时段保障** important period assurance

  提升服务级别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活动。

- **应急事件** emergency event

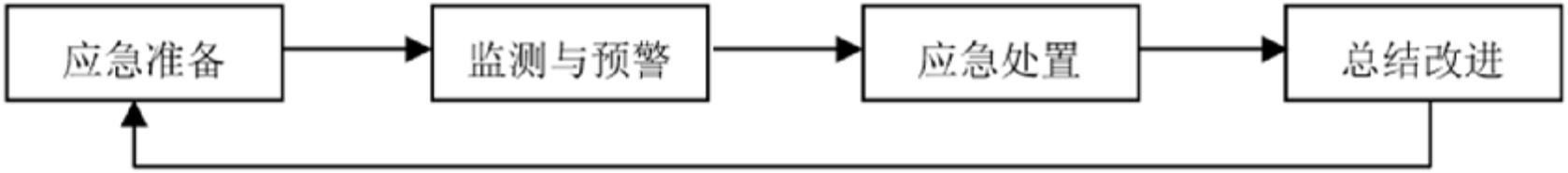
  导致或即将导致运行维护服务对象运行中断、运行质量降低，以及需要实施重点时段保障的事件。

- **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活动。

应急响应规范过程概述

- **本标准**规定了应急响应的基本过程和管理方法，并**将运行维护服务中应急响应过程划分为四个主要阶段：应急准备、监测与预警、应急处置和总结改进。**

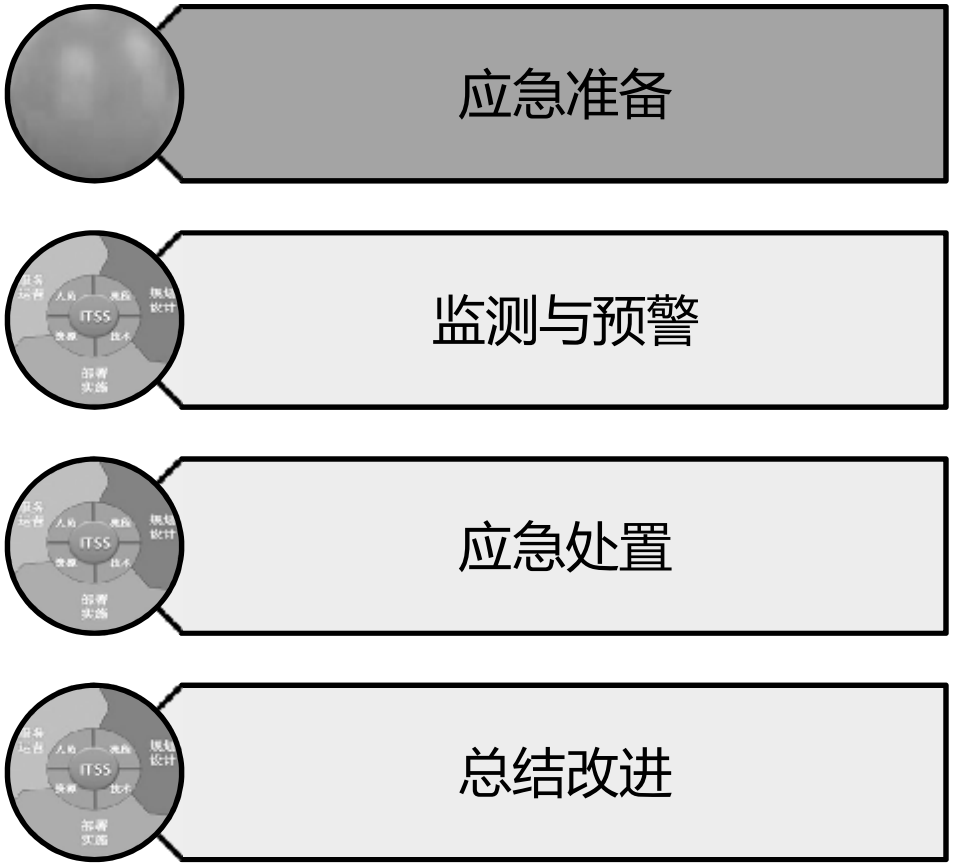


- **本标准国家标准号为：GB/T 28827.3，颁布日期为2012年11月5日**

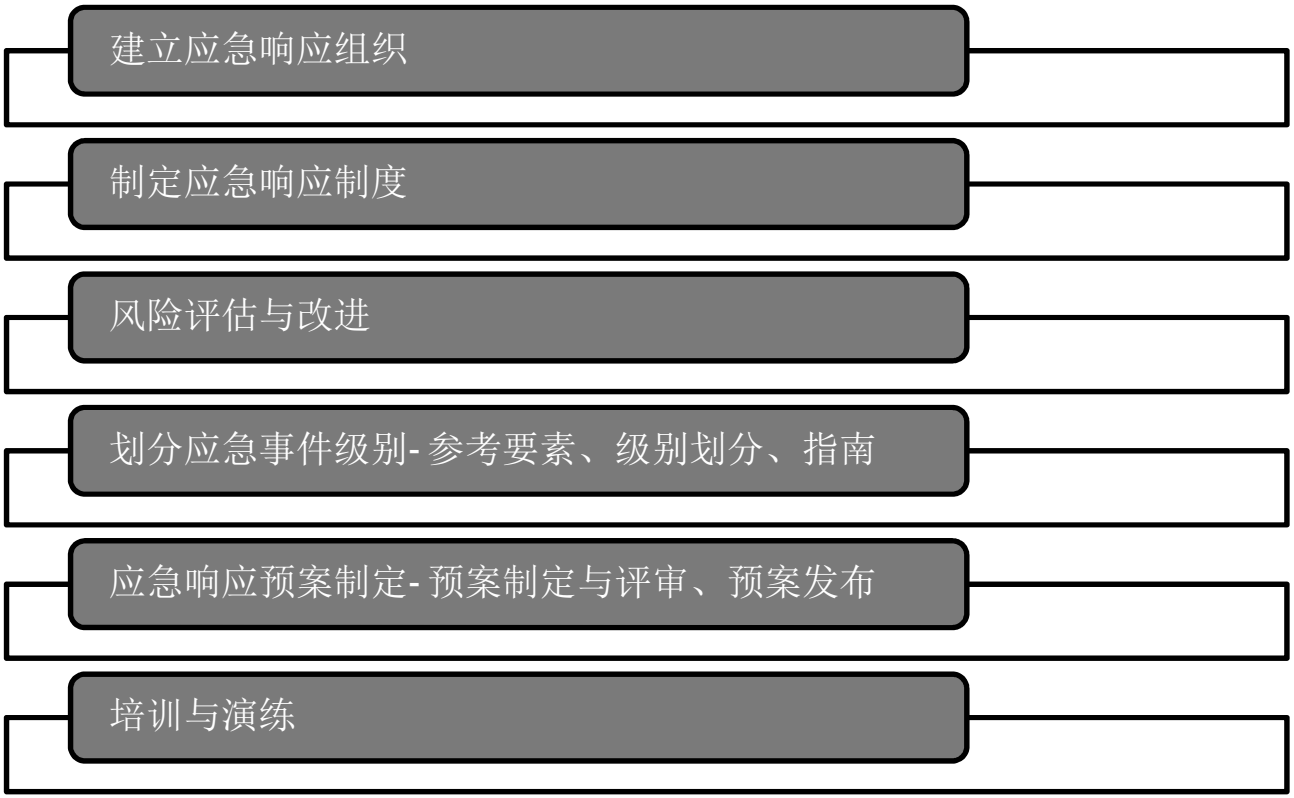
应急响应各阶段的工作内容

- **应急准备阶段的工作包括：组建应急响应组织，确定应急响应制度，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，定义应急事件级别，制定预案，开展培训和演练；**
- **监测与预警阶段的工作包括：进行日常监测，及时发现应急事件并有效预警，进行核实和评估，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，基于预案开展故障排查与诊断，对故障进行有效、快速的处理与系统恢复，及时通报应急事件，提供持续性服务保障，进行结果评价，关闭事件；**
- **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，持续改进应急工作，完善信息系统。**

应急响应阶段



应急准备活动


建立应急响应组织
制定应急响应制度
风险评估与改进
划分应急事件级别- 参考要素、级别划分、指南
应急响应预案制定- 预案制定与评审、预案发布
培训与演练

建立应急响应组织

- **运行维护服务的组织由相关利益方组成，包括服务需方、服务供方、分包方、供应商等。应在运行维护服务组织基础上建立应急响应组织，要求如下：**
  - ü **应急响应组织的人员应属于运行维护服务组织的人员，也可包括其他机构的专家和人员；**
  - ü **应规定运行维护服务及应急响应所有相关利益方的角色及职责，并为关键角色提供备份人选。应明确应急响应责任者、现场负责人、分组负责人、值班人员；**
  - ü **应就应急响应服务的范围、要求等与相关利益方达成一致，确定沟通流程和方式，并形成记录；**
  - ü **运行维护过程中涉及组织和人员的变更应与相关利益方达成一致，并形成记录；**
  - ü **应建立对应急响应组织内人员的考核机制，明确考核指标及方法。考核至少每年进行一次，以确保组织能持续满足应急响应要求。**

制定应急响应制度

- **组织应制定应急响应制度，明确应急响应的目标、原则、范围以及各项管理制度，并要求：**
  - ü **与相关利益方就应急响应制度达成一致；**
  - ü **定期对应急响应制度进行评审；**
  - ü **在组织战略、业务流程、客户要求等发生重大变化时对应急响应制度进行调整。**

风险评估与改进- 风险评估

- **组织应按照确定的方法和流程对重要信息系统实施风险评估，确保组织了解其在运行维护过程中的关键活动、所需资源、限制条件及信息系统面临的各种风险要素。组织应了解当风险演变为应急事件时所产生的影响和后果，以及信息系统服务中断所带来的损失。**
- **组织应授权组织内或组织外的服务供方进行风险识别，并将授权通知到所有相关利益方。**
- **被授权的服务供方应结合具体的信息系统现状和要求，从技术和管理等方面确定风险要素。**
- **应对风险要素进行评估，形成风险评估报告，报告内容应包括：**
  - **a）结论摘要；**
  - **b）背景及现状；**
  - **c）风险要素；**
  - **d）识别出的风险及风险分析；**
  - **e）建议的应对措施。**
- **应在需方授权范围内对风险评估报告进行评审和沟通，并达成一致。**

风险评估与改进- 改进

- **对于识别出的各种风险，组织应该制定明确的控制策略，必要时应对信息系统进行升级改造。可供选择的风险控制策略包括：风险规避、风险转移、风险降低、风险接受。**
- **根据风险评估报告，组织应该形成改进方案并实施，以利于：**

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。**

划分应急事件级别- 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、信息系统服务时段、信息系统受损程度。**

  a）重要程度

  重要程度主要应考虑信息系统所支撑的业务的重要性，以及信息系统内信息资产的重要性和信息系统服务的重要性。

  b）服务时段

  服务时段主要应考虑应急事件发生时系统提供服务的状态。

  c）受损程度

- **受损程度主要应考虑应急事件发生时信息系统功能和性能等方面的影响程度。**

划分应急事件级别- 级别划分

- **组织对可能发生的应急事件进行级别划分**
- **组织应结合自身的业务要求，对应急事件级别对应的响应时间、处置完成时间等达成一致**
- **组织应根据应急事件级别配置响应的保障措施，如人员、资金和设备等**

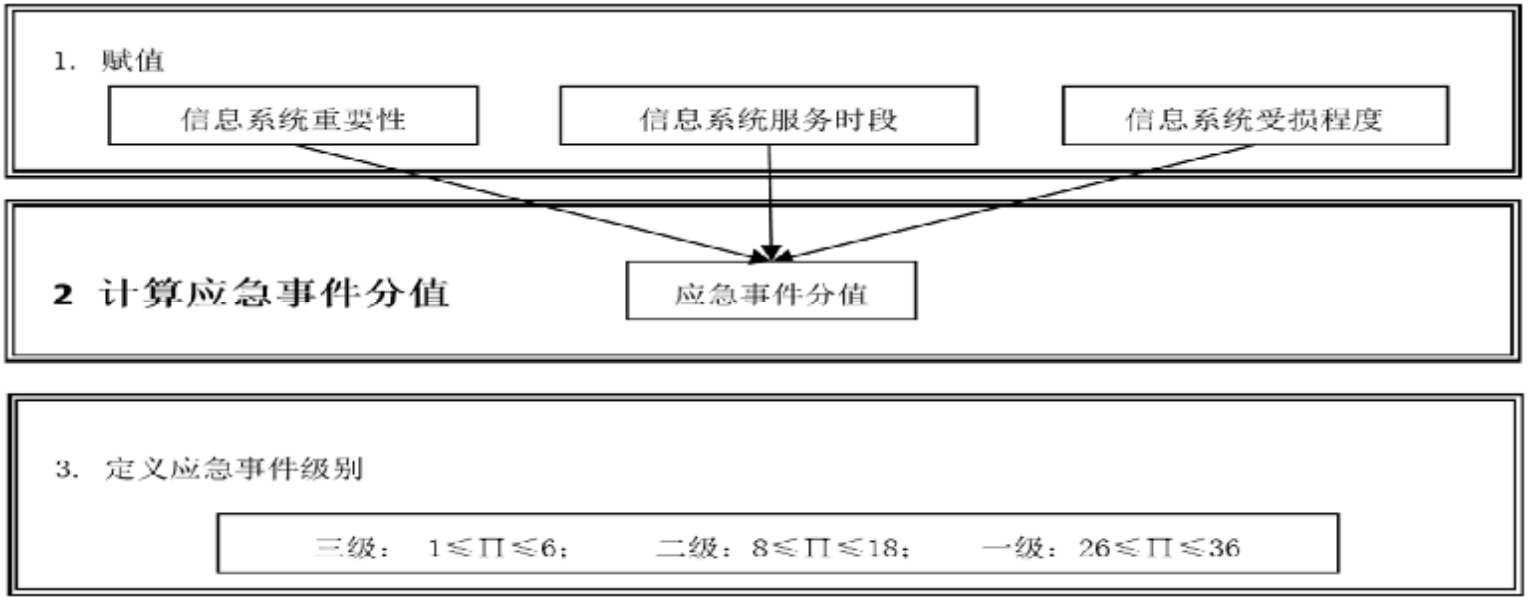
应急事件级别划分指南

参考要素的赋值

应急事件分级的主要参考要素为：信息系统的重要程度、信息系统服务时段、信息系统受损程度。

事件定级步骤

首先为应急事件的三个定级要素赋值，然后将三个要素赋值相乘，得到应急事件具体分值Π 。其范围在1～36。建议将分值在1～6区间的定义为三级事件，分值在8～18区间的定义为二级事件，分值在24～36区间的定义为一级事件。



应急响应预案制定- 预案制定与评审

- **组织应根据应急事件级别制定应急响应预案。**
- **应急响应预案可以分为总体预案和针对某个核心系统的专项预案。**
- **应急响应预案的格式应该能够为应急响应组织进行系统恢复操作提供快速明确的指导。**
- **应急响应预案应该明确、简洁，易于在紧急情况下执行，并使用检查列表。**
- **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）应急响应预案的启动；

  e）应急事件级别及对应的处置流程、方法；

  f）应急响应的保障措施；

  g）应急预案的附则。
- **服务需方应组织对应急响应预案进行评审，并与相关利益方达成一致。**

应急响应预案制定- 预案发布

- **经过评审确认的应急响应预案，应由应急响应责任者负责发布。**
- **应急响应预案应进行版本控制。**

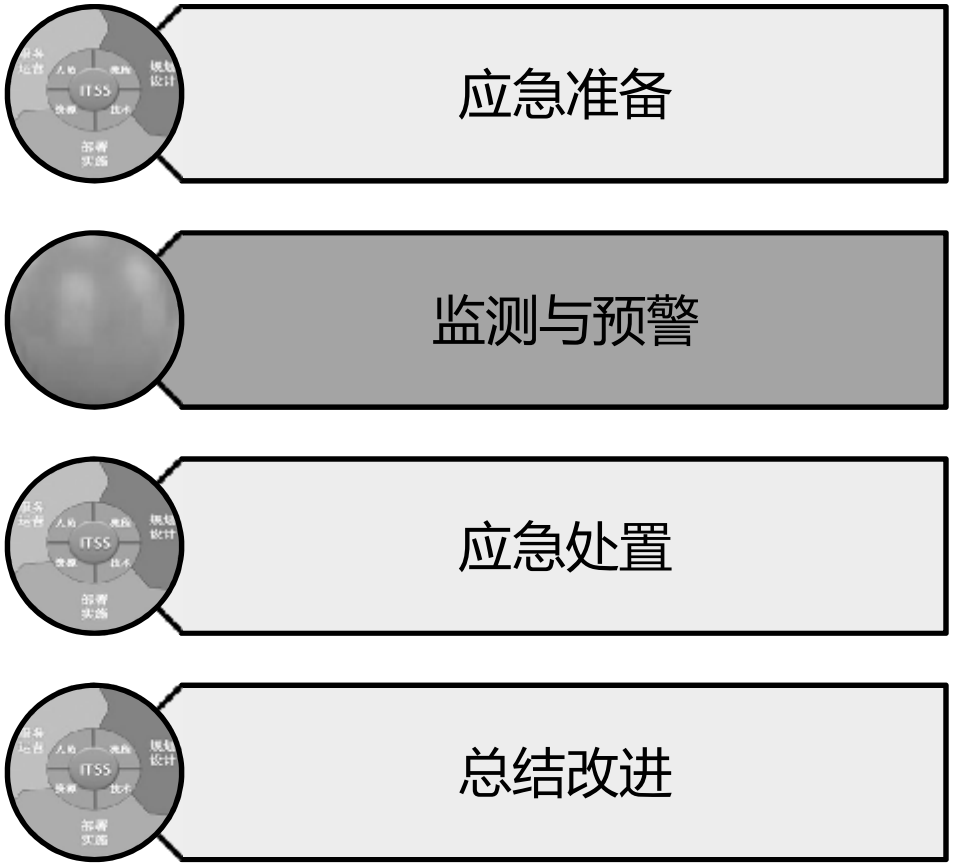
培训与演练- 培训

- **组织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。**
- **培训应至少每年举办一次。**

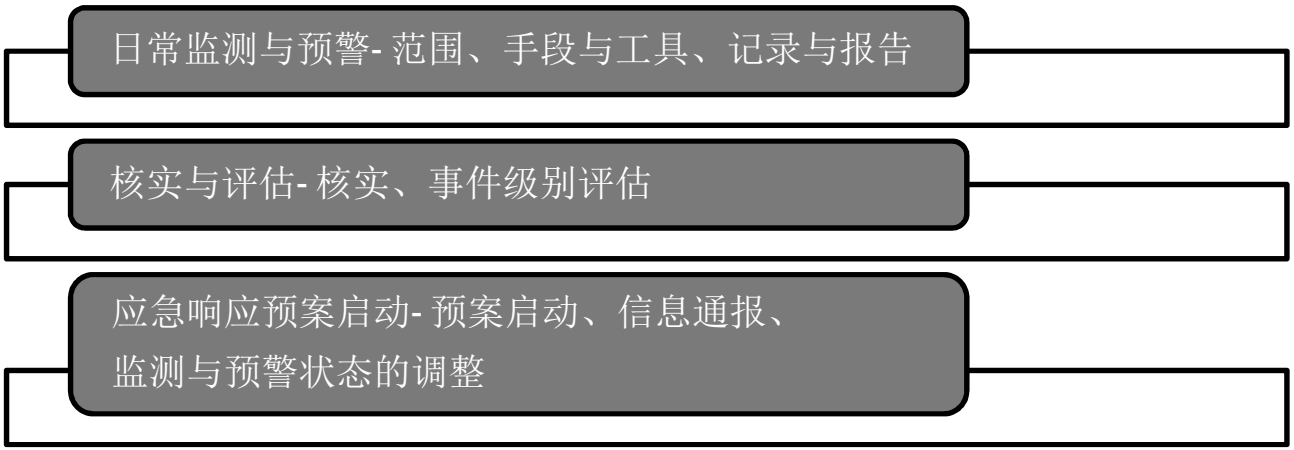
培训与演练- 演练

- **为检验应急响应预案的有效性，同时使相关人员了解运行维护预案的目标和内容，熟悉应急响应的操作规程，组织应进行应急演练，应：**
  - **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）演练不能影响业务的正常运行。**
- **为提升应急响应能力，组织可采用无脚本演练。**
- **必要时，组织可根据演练的效果，对应急响应预案进行完善。**

应急响应阶段



监测与预警活动


日常监测与预警- 范围、手段与工具、记录与报告
核实与评估- 核实、事件级别评估
应急响应预案启动- 预案启动、信息通报、
监测与预警状态的调整

日常监测与预警- 范围

- **组织应持续开展日常监测活动，实施有效预警，范围如下：**

a）组织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、终端等设备；

6）电力、空调、消防等基础环境。

b）组织应对信息系统所承载的业务数据进行监测，以跟踪和判别业务数据是否超出了预警条件。

日常监测与预警- 手段与工具

- **组织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) 建立知识库并保持更新；

c) 确定监测项、监测时间间隔与阈值；

d) 确定活动中的人员、角色和职责。

- **组织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。**

日常监测与预警- 记录与报告

- **组织应建立监测、预警的记录和报告制度，并按照约定的形式和时间间隔上报现场负责人。发现应急事件时，值班人员应提交报告，报告内容应包括：**
  - **a）应急事件发生及发现的时间、位置；**
  - **b）现象描述；**
  - **c）影响的范围；**
  - **d）初步原因分析；**
  - **e）报告人。**
- **报告应及时提交给现场负责人。报告方式包括电话、邮件、传真或书面文件等，并确认对方收到报告。**
- **值班人员应采取必要措施，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。**
- **应该对应急事件保持持续性跟踪。**

核实与评估- 核实

- **现场负责人应对报告内容进行逐项核实。**
- **核实确认后的应急事件报告，应提交给应急响应责任者。**
- **应急事件报告应作为事件级别评估的输入。**
- **重点时段保障需求也应作为事件级别评估的输入。**

核实与评估- 事件级别评估

- **现场负责人应根据事件级别定义，初步确定应急事件所对应的事件级别。**
- **应将事件级别置于动态调整控制中。**

应急响应预案启动- 预案启动

- **组织应建立、审议应急响应预案启动的策略和程序，以控制预案启动的授权和实施。**
- **组织应就应急响应预案启动可能造成的影响进行评估。**
- **相关利益方之间应就启动何种类型预案达成一致，包括当事件升级时，与之相对应的预案调整的方式。**
- **可根据先期处置要求进行应急响应预案的自动启动，或由应急响应责任者或现场负责人启动预案。**
- **应记录应急响应预案启动的过程和结果。**
- **重点时段保障应启动的应急响应预案可参考同级别预案确定。**

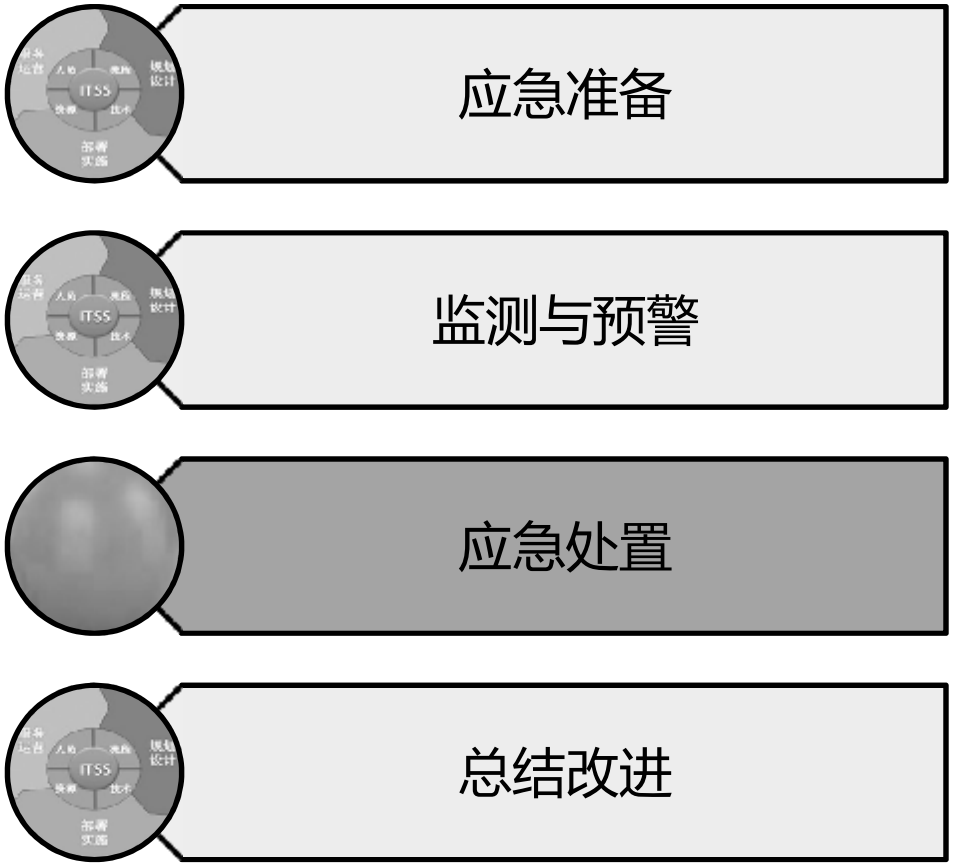
应急响应预案启动- 信息通报

- **现场负责人应向相关利益方通报应急响应预案启动信息，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措施或处置的目标；**
  - **e）实现目标所应采取的保障措施，如人员、资金和设备等；**
  - **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。**
- **信息通报应选取适当的方式，如电话、邮件、传真、书面文件等。**
- **所有相关利益方应对收到的通报信息进行确认和反馈。**

应急响应预案启动- 监测与预警状态的调整

- **通报信息应作为监测与预警状态调整的输入，调整内容包括监测范围、监测频率等。**
- **监测与预警状态的调整应通知各相关利益方。**

应急响应阶段



应急处置活动


应急调度
排查与诊断- 基本流程、问题沟通与确认
处理与恢复
事件升级- 升级、信息通报
持续服务
事件关闭- 申请、核实、调查和取证、关闭通报

应急调度

- **按照预案，开展统一的应急调度，包括人员、资金和设备等。**
- **应急调度中应：**

a) 获取现场信息；

b) 组织必要人员进行勘察、分析；

c) 下达调度命令并保持跟踪；

d) 保护可追查的相关线索。

排查与诊断- 基本流程

- **故障排查与诊断的流程应包含以下内容：**

a) **现场负责人调度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，必要时可寻求组织其他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现场负责人汇报故障排查情况、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。**

排查与诊断- 问题沟通与确认

- **处置过程中，现场负责人应及时与相关利益方进行沟通，沟通的内容主要包括系统故障点、造成故障的原因、排查诊断状况等。**
- **现场负责人应组织相关利益方对问题进行确认。**
- **问题确认过程不应延误处理与恢复工作的开展。**

处理与恢复

- **应基于应急响应预案、配置管理数据库、知识库等进行故障处理和系统恢复，处理与恢复的原则包括：**

a) **应在满足事件级别处置时间要求的前提下，尽快恢复服务；**

b) **采用的方法、手段不应造成次生、衍生事件的发生。**

- **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，并及时告知相关利益方。**
- **现场负责人应组织对处理与恢复的结果进行初步确认。**

事件升级- 升级

- **组织应建立、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。**
- **当实际处置时间超过事件级别处置时间要求时，应作为事件升级参考要素。**
- **组织应该对事件升级可能造成的影响进行评估，并在相关利益方之间达成一致。**
- **升级内容应包含预案调整、人员调整、资金调整以及设备调整。**
- **事件升级的实施授权应由现场负责人启动。**
- **应该对事件升级的过程和结果信息进行整理与归档。**

事件升级- 信息通报

- **现场负责人应向相关利益方通报事件升级信息，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) **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；**

e) **信息通报的范围和涉及的接受者。**

  - **信息通报应选择适当的方式，如电话、邮件、传真、书面文件等形式。**
  - **事件升级信息应作为处理与恢复的参考要素。**

持续服务

- **完成处理与恢复后，应组织运行维护人员提供持续性服务。**
- **组织应对持续性服务的效果进行评价。**
- **持续服务的评价结果，应作为应急事件关闭的输入。**

事件关闭- 申请

- **组织应建立、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进行整理。**
- **事件关闭申请应由相关的分组负责人提出，并提交相关文档资料。**
- **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。**

事件关闭- 核实

- **现场负责人接到事件关闭申请后，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。**

事件关闭- 调查和取证

- **当应急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）用作合同违约或其他纠纷的法律取证；**
  - **c）与相关方谈判赔偿事宜。**

事件关闭- 关闭通报

- **组织应建立、审议应急事件关闭通报制度。**
- **现场负责人应向相关利益方通报事件关闭信息，内容应包括：**

a) 事件发生的原因、事件级别及影响范围；

b) 事件对应的预案；

c) 事件的处置过程和方法；

d) 事件的调整升级情况；

e) 持续性服务情况；

f) 事件处置评价；

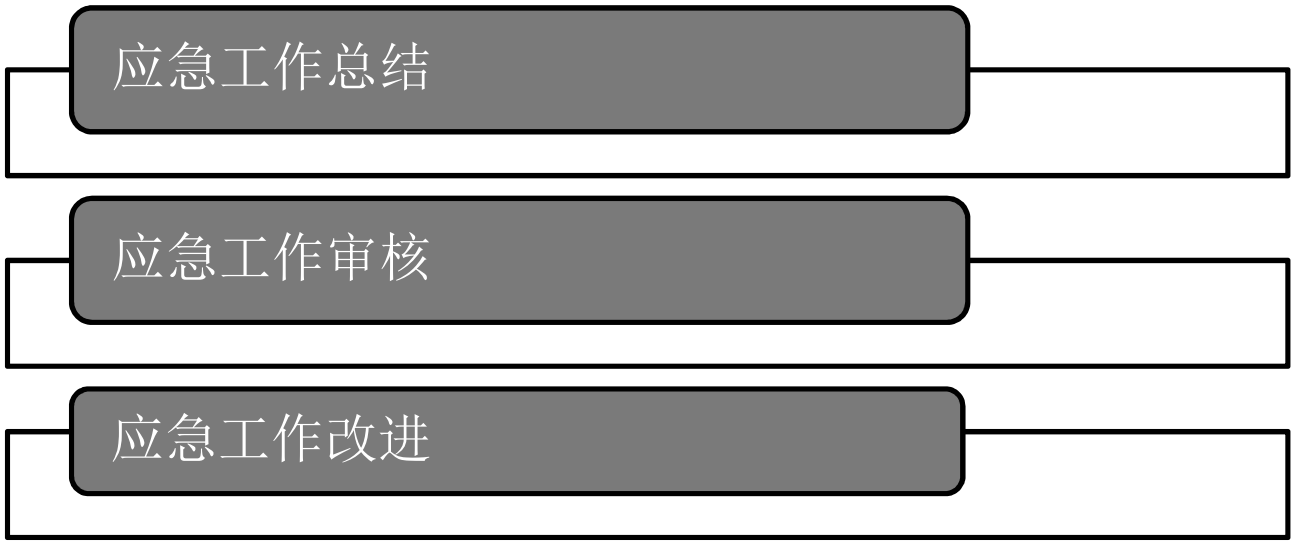
g) 事件关闭申请的处理意见；

h) 关闭通报的范围和涉及接受者。

- **应急事件发生的原因、处置过程和方法应记入知识库。**

应急响应阶段

总结改进活动



应急工作总结

- **组织应定期对应急响应工作进行分析和回顾，总结经验教训，并采取适当的后续措施。**
- **对应急响应工作的分析和回顾应考虑以下方面：**

  a）应急响应工作的绩效；

  b）应急准备工作的充分性和有针对性；

  c）应急事件发生原因、数量及频率；

  d）应急事件处置的经验得失；

  e）应急事件的趋势信息；

  f）信息系统中潜在的类似隐患。
- **对应急响应工作的分析和回顾应形成总结报告，并将总结报告作为改进应急响应工作及信息系统的重要依据。**

应急工作审核

- **为保证应急响应的有效性和时效性，应急响应责任者应定期组织对应急响应工作的评审，以确保应急响应过程和管理符合预定的标准和要求。审核的结果应该正式存档并通知给相关利益方。评审应至少每年举行一次。**

  a）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资源和流程；

  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）上次评审的后续活动跟踪；

  6）可能影响应急响应的各种业务变更；

  7）近期在处置应急事件过程中总结的经验和教训；

  8）培训的结果和反馈。

  b）审核的输出结果应该包括：

  1）改进目标；

  2）改进的具体工作内容；

  3）所需的各种资源，包括人员、资金和设备等。

应急工作改进

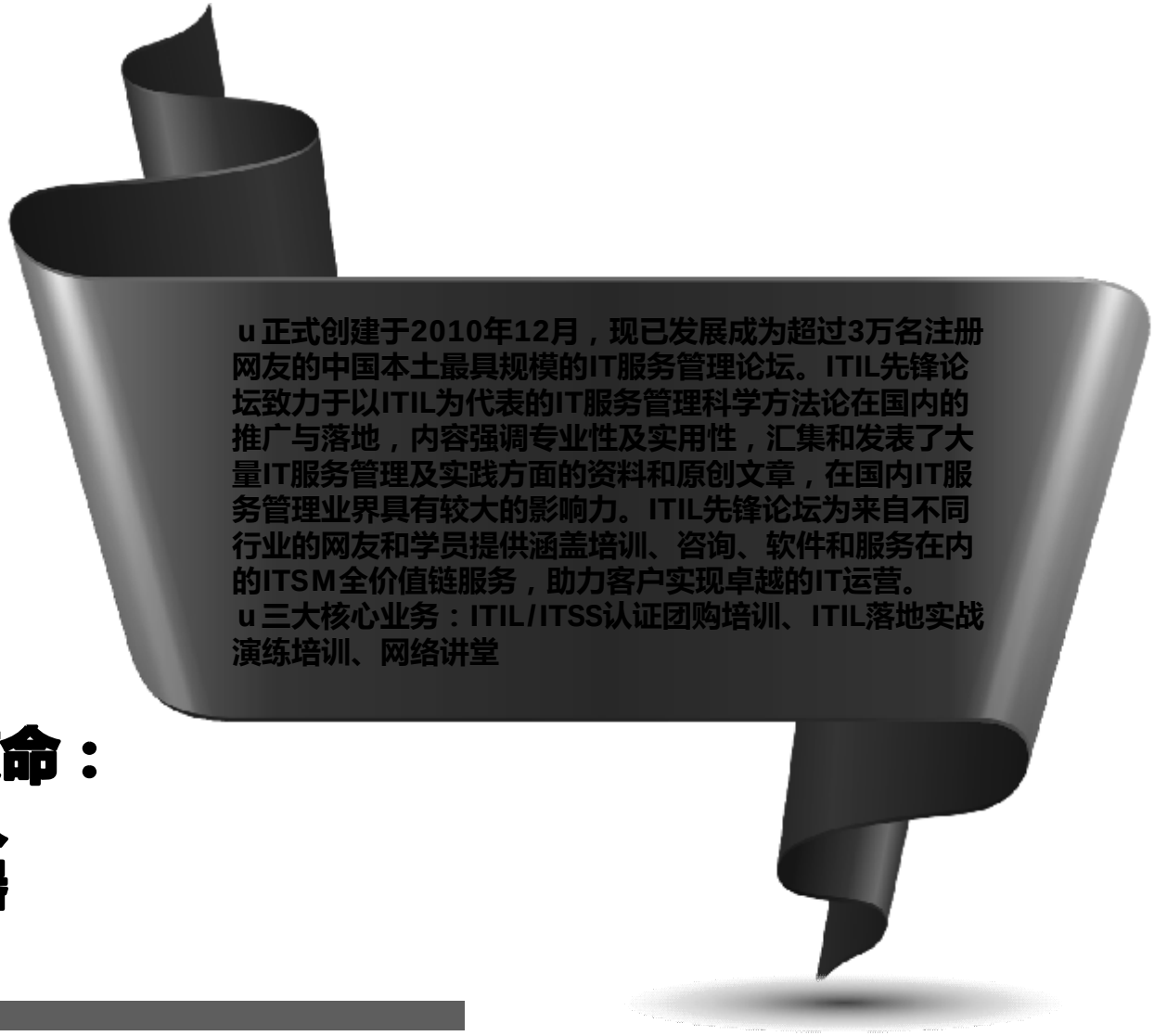
- **应急事件总结、应急工作审核的结果应该作为应急准备阶段各项工作的改进要素。组织应根据总结报告中给出的建议项和评审结果，完善信息系统，深化应急准备工作。**

不同类型活动与重点任务的对应关系

应急响应各阶段工作内容与日常工作、故障响应、重点时段保障等各类型活动的对应关系

主要阶段	工作内容	日常工作	故障响应	重点时段保障
应急准备	建立应急响应组织	√		
	制定应急响应制度	√		
	风险评估与改进	√		
	划分应急事件级别	√		
	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		√	
	事件升级		√	√
	持续服务		√	√
	事件关闭		√	√
总结改进	应急工作总结		√	√
	应急工作审核		√	√
	应急工作改进	√	√	√

ITIL先锋论坛



u正式创建于2010年12月，现已发展成为超过3万名注册网友的中国本土最具规模的IT服务管理论坛。ITIL先锋论坛致力于以ITIL为代表的IT服务管理科学方法论在国内的推广与落地，内容强调专业性及实用性，汇集和发表了大量IT服务管理及实践方面的资料和原创文章，在国内IT服务管理业界具有较大的影响力。ITIL先锋论坛为来自不同行业的网友和学员提供涵盖培训、咨询、软件和服务在内的ITSM全价值链服务，助力客户实现卓越的IT运营。

u三大核心业务：ITIL/ITSS认证团购培训、ITIL落地实战演练培训、网络讲堂

我们的宗旨与使命：

- ✓ ITIL初学引路人
- ✓ ITIL落地推进器
- ✓ ITSM交流门户

Thanks.