ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38645—2020

信息安全技术　网络安全事件应急演练指南

Information security techniques—Guide for cybersecurity incident emergency exercises

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:烽台科技(北京)有限公司、国家工业信息安全发展研究中心、国家电网有限公司、国家信息技术安全研究中心、中国证监会信息中心、中国电力科学研究院有限公司、中国电子技术标准化研究院、黑龙江省工业和信息化厅、清华大学、北京京航计算通讯研究所、北京理工大学、哈尔滨工业大学、哈尔滨工程大学、桂林电子科技大学、公安部第三研究所、中国信息安全测评中心、国家计算机网络应急技术处理协调中心、中国互联网络信息中心、中国科学院信息工程研究所、中国电子科技网络信息安全有限公司、黑龙江省电子技术研究所、北京启明星辰信息安全技术有限公司、哈尔滨工大天创电子有限公司、国网山东省电力公司电力科学研究院、北京安天网络安全技术有限公司、北京网藤科技有限公司、哈尔滨工业大学软件工程股份有限公司、黑龙江信息技术职业学院、北京市政务信息安全应急处置中心、北京网御星云信息技术有限公司、北京卓识网安技术股份有限公司。

本标准主要起草人:龚亮华、尹丽波、王磊、宫亚峰、刘莹、王东明、张格、刘迎、朱朝阳、魏钦志、周亮、李琳、张永静、张洪、李俊、于盟、王达、薛一波、祝烈煌、王佰伶、孙建国、丁勇、佟薇薇、孙立立、王启蒙、雷承霖、赵旭东、邱梓华、邹春明、贾若伦、訾立强、谢丰、杜红亮、何能强、李若愚、郝志宇、敖佳、刘慧晶、郑显生、孟雅辉、刘文跃、王文婷、李柏松、童志明、李佐民、郭宇亮、左晓英、范士喜、张涛、魏彬、杜君、刘健帅、刘韧。

引　言

建立网络安全事件应急工作机制，开展应急演练是减少和预防网络安全事件造成损失和危害的重要保证。为规范和指导网络安全事件应急演练工作，制定网络安全事件应急演练指南是必要的。

信息安全技术　网络安全事件应急演练指南

1　范围

本标准给出了网络安全事件应急演练实施的目的、原则、形式、方法及规划，并描述了应急演练的组织架构以及实施过程。

本标准适用于指导相关组织实施网络安全事件应急演练活动。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069　信息安全技术　术语

3　术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

网络安全事件　cybersecurity incident

由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

3.2

网络安全事件应急演练　cybersecurity incident emergency exercises

有关政府部门、企事业单位、社会团体组织相关人员，针对设定的突发事件模拟情景，按照应急预案所规定的职责和程序，在特定的时间和地域，开展应急处置的活动。

4　应急演练目的

应急演练目的如下：

a) 检验预案：通过开展应急演练，查找和验证应急预案中存在的问题，完善应急预案，提高应急预案的科学性、实用性和可操作性；

b) 完善准备：通过开展应急演练，检查应对网络安全事件所需应急队伍、物资、装备、技术等方面的准备情况，发现不足及时予以调整补充，做好应急准备工作；

c) 锻炼队伍：通过开展应急演练，增强演练管理部门、指挥机构、参演机构和人员等对应急预案的熟悉程度，锻炼应急处置需要的技能，加强配合，提高其应急处置能力；

d) 磨合机制：通过开展应急演练，进一步明确相关单位和人员的职责任务，理顺工作关系，完善各关联方之间分离、阻隔、配套应急联动机制，防范网络安全风险传导；

e) 宣传教育：通过开展应急演练，普及应急知识，不断增强网络安全管理的专业化程度，提高全员网络安全风险防范意识。

5 应急演练原则

应急演练原则如下：

a) 结合实际：结合应急管理工作要求，明确演练目的，根据资源条件确定演练方式和规模；

b) 贴合实战：提高应急指挥机构的指挥协调能力和应急队伍的实操应急处置能力；

c) 提高实效：重视对演练流程及演练效果的评估、考核，总结推广经验，整改发现的问题；

d) 保证安全：围绕演练目的策划演练内容，科学制定演练方案，部署演练活动，制定并遵守有关安全措施，确保演练参与人员及演练设施安全；

e) 统筹规划：统筹规划应急演练活动，演与练有效互补，适当开展跨行业、跨地域的综合性演练，利用现有资源，提升应急演练效益。

6 应急演练形式

按照应急演练的组织形式、内容、目的和作用的不同，应急演练形式可以从多个维度进行划分：

a) 按照应急演练的组织形式，分为如下形式：

1) 桌面推演：参演人员根据应急预案，利用流程图、计算机模拟、视频会议等辅助手段，针对事先假定的演练场景进行模拟应急决策及现场处置的过程，验证应急预案的有效性，促进相关人员明确应急预案中有关职责，掌握应急流程及应急操作，提高指挥决策和各方协同配合能力。

2) 模拟演练：参演人员利用网络与信息系统相关软硬件或靶场技术，模拟构建接近真实环境的测试环境，模拟突发事件场景或场景片段，注重模拟演练技术操作的验证、演练过程中各方资源的协调和配合、演练过程中各类问题和风险的应对。

3) 实操演练：参演人员利用网络与信息系统真实环境模拟突发事件场景，完成判断、决策、处置等环节的应急响应过程，检验和提高相关人员的临场组织指挥、应急处置和后勤保障能力。实操演练还可分为指定科目演练和预先不告知科目演练。

b) 按照应急演练的内容，分为如下形式：

1) 专项演练：指涉及应急预案中特定系统或应急响应功能的演练活动。针对一个或少数几个参与部门(岗位)的特定环节和功能进行检验。

2) 综合演练：指涉及应急预案中多项或全部应急响应功能的演练活动。对多个环节和功能进行检验。

c) 按照应急演练的目的和作用，分为如下形式：

1) 检验性演练：为检验应急预案的可行性、应急准备的充分性、应急机制的协调性及相关人员的应急处置能力而组织的演练。

2) 示范性演练：为向观摩人员展示应急能力或提供示范教学，按照演练方案开展的表演性演练。

3) 研究性演练：为研究和解决突发事件应急处置的重点、难点问题，试验新方案、新技术、新装备而组织的演练。

d) 其他演练形式。

不同维度的演练相互组合，可以形成专项桌面推演、综合性桌面推演、专项实操演练、综合性实操演练、专项示范演练、综合性示范演练等常用演练形式，常用演练形式参见附录 A。

7 应急演练规划

有关组织根据实际情况，依据相关法律法规、应急预案的规定和管理部门的要求，对一定时期内各类应急演练活动做出总体规划，包括应急演练的频次、规模、形式、时间、地点、预算等。一般以一年为一个周期制定演练规划。

8 应急演练组织架构

8.1 综述

演练组织架构包括管理部门、指挥机构和参演机构。根据事件等级、演练规模、演练目的、演练形式等，组织机构可对相关机构人员和职责进行归并等调整，按实际情况进行相应组织细分。

8.2 管理部门

管理部门包括上级单位、国家有关网络安全监管部门等，主要职责如下：

a) 下发应急演练要求；
b) 审批或备案下级组织单位应急演练规划；
c) 必要情况下，宣布应急演练开始、结束或终止。

8.3 指挥机构

8.3.1 指挥人员

主要职责如下：

a) 对应急演练工作的承诺和支持，包括发布正式文件、提供必要资源（人、财、物）等；
b) 审核并批准应急演练方案；
c) 审批决定应急演练重大事项；
d) 部署、检查、指导和协调应急演练各项筹备工作；
e) 负责跨组织、跨领域应急演练的各项协调工作；
f) 对外联络相关单位，协调各单位在应急演练中的职责；
g) 指挥、调度应急演练现场工作；
h) 宣布应急演练开始、结束或终止；
i) 总结应急演练效果、完成演练总结报告；
j) 跟踪演练成果运用。

8.3.2 策划人员

主要职责如下：

a) 策划、制定应急演练方案；
b) 负责应急演练过程中的解说。

8.3.3 督导人员

主要职责如下：

a) 督查演练活动是否符合应急演练规划要求；
b) 现场监督指导应急演练具体工作。

8.4 参演机构

8.4.1 顾问人员

由演练组织单位牵头相关参演机构领导及技术专家组成，在演练实施阶段赴各参演机构演练现场指导演练工作。

8.4.2 实施人员

主要职责如下：

a) 执行演练脚本；
b) 按照应急预案对模拟触发的网络安全事件进行应急响应处置；
c) 对不设场景的预案模拟触发的网络安全事件进行实战应急响应处置；
d) 运用演练成果。

8.4.3 保障人员

主要职责如下：

a) 跟踪拟定演练人员按要求参与演练活动；
b) 负责调集演练过程需要的各项器材，并准备好通信、调度等技术支撑系统；
c) 落实演练场地、物资，开展后勤保障工作；
d) 跟踪、落实演练规划中要求的经费；
e) 负责演练现场的安全保障工作。

8.4.4 技术支持人员

主要职责如下：

a) 为应急演练活动提供应急技术、演练技术咨询与支撑；
b) 调试演练过程需要的各项器材，并做好通信、调度等技术支撑系统的技术保障工作；
c) 负责应急演练各环节包括监测、处置等环节的具体技术实现；
d) 模拟触发网络安全事件。

8.4.5 评估人员

主要职责如下：

a) 记录演练过程与应急动作要领；
b) 评价演练效果、演练过程及动作要领，完成演练评估报告；
c) 发现应急演练中存在的问题，及时向相关职责人员提出意见或建议。

8.4.6 其他人员

主要职责如下：

a) 对外联络其他参演机构，协助完成应急演练工作；
b) 协调跨组织、跨领域参演人员完成应急演练工作；
c) 特邀相关单位领导及其他各类人员，观察演练过程等；
d) 负责应急演练的其他工作。

9 应急演练实施过程

9.1 准备阶段

9.1.1 制定演练计划

9.1.1.1 综述

应急指挥机构根据应急演练规划和应急预案制定演练计划，明确演练目的，分析演练要求，确定演练范围，起草日程计划，编制演练经费预算。应急演练计划模板参见附录 B 的 B.1。

9.1.1.2 明确演练目的

明确开展应急演练的原因、演练要解决的问题和期望达到的效果。

9.1.1.3 分析演练要求

根据应急演练规划和应急预案要求，在对事先设定事件场景风险和应急预案认真分析的基础上，结合年度内发生网络安全事件的情况，发现存在的问题和薄弱环节，确定需调整的演练人员、需锻炼的技能、需检验的设备、需完善的应急处置流程、指挥调度程序以及需进一步明确的职责等，分析完成举办应急演练的要求。

9.1.1.4 确定演练范围

根据演练要求以及综合场地、资源（包括但不限于人力资源、财力资源、物力资源、技术资源、信息资源等）和时间等制约条件和因素，确定演练背景事件类型、等级、发生地域、演练组织架构（管理部门、指挥机构和参演机构）及人数、演练方式等。演练要求和演练范围往往互为影响。

9.1.1.5 起草日程计划

起草演练工作计划及日程，细化确定应急演练各阶段的主要任务和完成时限，包括各种演练文件编写与审定的期限、信息系统及技术物资准备的期限、演练实施的日期等。

9.1.1.6 编制演练经费预算

编制开展演练活动的各项经费、配套经费及保障措施。

9.1.2 制定演练方案

9.1.2.1 编制工作方案

编制应急演练工作方案的步骤如下：

a） 确定目标

演练目标是需完成的主要演练任务及其达到的效果，一般说明“由谁在什么条件下完成什么任务，依据什么标准，取得什么效果”。演练目标应明确、具体、可量化、可实现。如一次演练有若干项演练目标，每项演练目标都要在演练方案中有相应的事件和演练活动予以实现，并在演练评估中有相应的评估项目判断该目标的实现情况。

b） 设计演练场景和实施步骤

演练场景宜为演练活动提供初始条件，还要通过一系列的情景事件引导演练活动继续，直至演练完成，演练场景库参见附录 C。演练场景包括如下的演练场景概述和演练场景清单：

1） 演练场景概述。每一处演练场景的概要说明，宜说明事件类别、发生的时间地点、发展速度、受影响范围、人员和物资分布、已造成的损失、后续发展预测等。

2） 演练场景（步骤）清单。要明确演练过程中各场景（各步骤）的时间顺序列表和耗时情况。演练场景之间的逻辑关联依赖于事件发展规律、控制消息和演练人员收到控制消息后应采取的行动。

c） 拟定演练人员名单

应急演练的参演机构统一成立应急演练指挥机构。由指挥机构发起演练活动的，应急演练的应急指挥机构宜向管理部门备案。根据演练的形式、内容、组织范围等实际情况，演练组织机构和职能可适当调整。

演练活动应在指挥机构的督导、指挥下开展。

d） 编写工作方案

应急演练工作方案内容宜包括：指导思想、工作原则、演练目的、演练场景、演练时间地点、指挥机构和参演机构、角色职责、演练实施过程、其他准备事项、工作要求及有关附件等，模板参见 B.2。

9.1.2.2 编制保障方案

在编制演练保障方案时，从人员保障、经费保障、场地保障、基础设施保障、通信保障、技术保障、安全保障等方面制定详细、可行的方案，理清责任归属，科学预测演练活动过程中可能发生的意外或故障，制定相应意外或故障处理流程、措施等，模板参见 B.3。

9.1.2.3 编制评估方案

演练评估是通过观察、体验和记录演练活动，比较演练实际效果与目标之间的差异，总结演练成效和不足的过程。演练评估宜以演练目标为基础。每项演练目标都要设计合理的评估项目方法、标准。根据演练目标的不同，可以用选择项（如：是/否判断，多项选择）、主观评分（如：1——差、3——合格、5——优秀）、定量测量等方法进行评估。

为便于演练评估操作，策划组通常事先设计好评估表格，包括演练目标、评估方法、评价标准和相关记录项等，也可采用专业评估软件等工具，模板参见 B.4。

9.1.2.4 编写演练脚本

根据应急演练目的、内容和形式编制应急演练脚本。应急演练脚本是应急演练工作方案的具体操作手册，控制应急演练时间进程，对应急演练场景和响应程序进行详细说明，一般采用表格形式，以应急演练流程的各关键节点为骨干，描述应急演练的场景、起止时间、执行人员、处置行动、指令与对白、适时选用的技术设备、视频画面与字幕、解说词等，模板参见 B.5。

9.1.3 评审与修订演练方案

对演练方案进行评审，确定演练方案科学可行，以确保应急演练工作的顺利进行。对涉密或不宜公开的演练内容，宜制订保密措施。

应急演练方案的制定可参考附录 D。

9.1.4 应急演练保障

9.1.4.1 人员保障

保证相关人员参与演练活动的时间，确保所有参演人员已经通过演练培训，明确职责分工。

9.1.4.2 经费保障

每年宜根据应急演练规划编制应急演练的经费预算，纳入各参演机构的年度财政（财务）预算，并按照演练需要及时拨付经费。对经费使用情况进行监督检查，确保演练经费专款专用、节约高效。

9.1.4.3 场地保障

根据演练方式和内容，在经现场勘察后选择合适的演练场地。桌面推演一般可选择会议室或应急指挥中心等；实操演练宜选择与实际情况相似的机房或地点。

9.1.4.4 基础设施保障

提供必要的基础设施保障，包括但不限于电力、设备、物资、通信器材等。

9.1.4.5 通信保障

为应急演练过程提供及时可靠的信息传递渠道。根据演练需要，可以采用多种公用或专用通信系统，必要时可组建演练专用通信与信息网络，确保演练控制信息的快速传递。

9.1.4.6 技术保障

根据应急演练方案，预先设计技术保障方案，保障应急演练所涉及的各类技术支撑系统的正常运转。当工作流程发生变化后，技术保障方案也需相应进行调整。

根据组织的网络和信息系统类型，宜储备应急演练需要的漏洞、补丁等技术资源，并对技术资源进行合理的调配和使用。在对攻防工具、脚本等危险性技术资源的储备、调配和使用中，宜进行合理的安全风险管控。

9.1.4.7 安全保障

充分考虑演练全过程的安全保障风险，尤其是大型或高风险演练，宜制定专门应急预案，采取预防措施，并对关键部位和环节可能出现的突发事件进行专项安全保障。

对可能影响公众生活、易于引起公众误解和恐慌的应急演练（特别是可能造成业务中断的演练），宜提前向社会发布公告，告示演练内容、时间、地点和组织单位，并做好应对方案，避免造成负面影响。

演练过程中涉及敏感系统的，宜满足相关保密要求。在做好数据备份的基础上，对其中的敏感数据应事先进行脱敏处理；在演练方案设计时，宜充分考虑在演练中可能突破其原有对敏感信息访问权限的人员及由此可能造成的后果。

演练现场宜有必要的安保措施，必要时对演练现场进行封闭或管制，保证演练安全进行。演练出现意外情况时，及时报告并批准后，提前终止演练。

9.1.4.8 保障检查

演练正式启动前，组织单位宜开展如下充分的保障检查：

a） 检查参演人员到位情况；

b） 检查演练方案中各项保障资源准备情况，确保各项保障措施到位；

c） 检查参演系统配置和数据备份正确和完备，检查演练所需的工具、设备、设施、技术资料到位；

d） 应对应急演练所用各类设施、设备进行全面检查和调试，保证处于正常工作状态；

e） 其他保障检查工作。

参演机构完成保障检查后，向指挥机构确认。

9.1.5 演练动员与培训

在演练开始前宜组织演练动员和培训，确保所有参演人员已熟练掌握演练规则、演练情景，明确各自在演练中的职责分工。

9.1.6 应急演练预演

为保证正式应急演练效果，宜在前期培训的基础上，在演练正式开始前安排一次或多次预演。对于大型综合性实操演练，可按照先易后难、先分解后合练、循序渐进的原则，采取分阶段推演形式，检查验证应急演练的局部或全部工作环节，强化参演机构与人员的协同配合意识，查找问题和不足，持续改进提升应急演练方案。为演练的成功举行奠定基础。

9.2 实施阶段

9.2.1 演练启动

检查演练各环节准备到位后，由管理部门派员或指挥机构宣布演练开始，启动演练活动。

对演练实施全过程的指挥控制，随时掌握演练进展情况，按照演练方案要求对安全事件的发现及处置进展情况向指挥机构报告。

视情对演练过程进行解说。解说内容宜包括演练背景描述、进程讲解、案例介绍、环境渲染等。

各参演机构按照演练方案开始进行应急演练。

9.2.2 安全事件模拟

演练实施过程中，根据演练指令，按照演练方案开展安全事件模拟。安全事件模拟分为如下现象模拟和机理模拟：

a) 现象模拟：通过可控的方法复现出安全事件在设备、网络、服务等方面表现出的现象；

b) 机理模拟：在演练场景中通过可控的方式真实触发安全事件。

9.2.3 演练执行

9.2.3.1 综述

安全事件演练执行具体步骤分为监测预警、事件研判、事件通告、事件处置、系统确认五个阶段。

9.2.3.2 监测预警

实时监测风险信息，将有效信息上报；组织专家进行研判，根据应急预案的要求，确定预警等级，发布预警信息。

9.2.3.3 事件研判

监测或直接发现安全事件，宜对安全事件进行评估，确定安全事件的类别、级别，启动安全事件全面监测措施。

9.2.3.4 事件通告

根据演练场景要求模拟进行组织内信息通报、组织外信息通报、信息上报和信息披露。

9.2.3.5 事件处置

宜依据安全事件发展态势，快速分析评估安全事件，形成处置方案。现场处置方案宜参考安全事件

应急预案，并依据具体情况做适当选择。

依据处置方案，实施现场应急处理，消除网络安全隐患及威胁，抑制安全事件影响。

依据处置方案，实施恢复操作。恢复操作宜包括建立临时业务处理能力、修复原系统的损害、在原系统或新设施中恢复运行业务能力等应急措施。实施组恢复复杂系统时，恢复顺序宜反映出系统允许的中断时间，以避免对相关系统及业务的重大影响。

9.2.3.6 系统确认

确认参演系统恢复正常并向指挥机构报告，模板参见 B.6。

9.2.4 演练记录

演练实施过程中，评估人员按照演练方案采用文字、脚本、照片和音像等手段开展评估素材采集。

文字记录宜包括演练实际开始与结束时间、演练过程控制情况、各项演练活动中参演人员的表现、意外情况及其处置等内容。脚本宜包括应急处置效果验证和处置现场数据的采集等内容。照片和音像记录应在不同现场、不同角度进行拍摄，尽可能全方位反映演练实施过程，模板参见 B.7。

9.2.5 演练结束与终止

网络安全事件处置结束后，指挥机构宣布演练执行过程结束，所有人员停止应急处置活动。在确认参演系统恢复正常后，指挥机构做简短总结，宣布演练实施阶段结束，并对演练过程进行点评。

演练实施过程中出现下列情况，经指挥机构或管理部门决定，可提前终止演练：

a) 出现真实突发事件，需要参演人员参与应急处置时，要终止演练，使参演人员迅速回归其工作岗位，履行应急处置职责；

b) 出现特殊或意外情况，短时间内不能妥善处理或解决时，可提前终止演练。

9.3 评估与总结阶段

9.3.1 演练评估

分析演练记录及相关资料，对演练活动及组织过程做出客观评价，编写演练评估报告。

演练评估通过组织评估会议、填写演练评价表和对参演人员进行访谈等方式进行，对演练效果及演练的整体流程进行评估，提出完善建议。可要求参演机构提供自我评估总结材料，收集演练组织实施的情况。

演练评估报告的主要内容包括演练执行情况、演练方案的合理性与可操作性、应急指挥人员的指挥协调能力、参演人员的处置能力、演练所用设备装备的适用性、演练目标的实现情况、演练的成本效益分析、对完善预案的建议等，模板参见 B.8。

9.3.2 演练总结

根据演练记录、演练评估、演练方案等材料，对演练进行系统和全面的总结，并形成演练总结报告。参演机构可对本单位的演练情况进行总结。

演练总结报告的内容包括：演练目的，时间和地点，参演机构和人员，演练方案概要，发现的问题与原因，经验和教训，以及改进有关工作的建议等，模板参见 B.9。

9.3.3 文件归档与备案

将演练计划、演练方案、演练评估报告、演练总结报告等资料归档保存。对于由管理部门布置或参与的演练，或者法律、法规、规章要求备案的演练，宜将相关资料报有关部门备案。

9.3.4 考核与奖惩

对演练参与人员进行考核。对在演练中表现突出的工作组和个人，可给予表彰和奖励；对不按要求参加演练，或影响演练正常开展的个人，可给予相应批评。

考核与奖惩应纳入绩效考核体系。

9.4 成果运用阶段

9.4.1 改善提升

指挥机构宜根据演练评估报告、演练总结报告提出的问题和建议对应急处置工作进行持续改进。指挥机构宜制定整改计划，明确整改目标，确定整改措施，落实整改资金。

9.4.2 监督整改

指挥机构宜指派专人监督检查整改计划执行情况，确保演练评估报告、演练总结报告提出的问题和建议得到及时整改。

附 录 A
（资料性附录）
常用演练形式对照表

常用演练形式对照表见表 A.1。

表 A.1 常用演练形式对照表

演练对象	专项桌面推演	专项实操演练	专项示范演练	综合性桌面推演	综合性实操演练	综合性示范演练
组织	适用范围：适用于根据各机构自身年度演练计划，由机构层面统一牵头，或某部门发起的涉及机构其他有关部门的、针对某一专项应急功能设置的演练场景	适用范围：适用于根据各机构自身年度演练计划，由机构层面统一牵头，或某部门发起的涉及机构其他有关部门的、针对某一专项应急功能设置的演练场景	适用范围：适用于根据各机构自身年度演练计划，由机构层面统一牵头，或某部门发起的涉及机构其他有关部门的、针对某一专项应急功能设置的演练场景	适用范围：适用于根据各机构自身年度演练计划，由机构层面统一牵头、覆盖机构所有部门及成员的、针对可能导致机构核心业务中断引发全局性风险事件设置的场景	适用范围：适用于根据各机构自身年度演练计划，由机构层面统一牵头、覆盖机构所有部门及成员的、针对可能导致机构核心业务中断引发全局性风险事件设置的场景	适用范围：适用于根据各机构自身年度演练计划，由机构层面统一牵头、覆盖机构所有部门及成员的、针对可能导致机构核心业务中断引发全局性风险事件设置的场景
	目的：通过桌面推演完善机构内部应急指挥、决策和应急处置机制，落实安全责任制，检验有关专项应急预案有效性，促进相关人员深入掌握应急预案，完善应急准备	目的：通过实操演练磨合机构内部应急指挥、决策和应急处置机制，检验有关专项应急预案中各项应急操作流程的有效性、可执行性，培养有关人员的临场应变能力	目的：通过示范演练提示风险，切实提升机构领导层对网络安全事件应急演练的重视程度；促进机构内部应急工作交流	目的：通过桌面推演完善机构内部应急指挥决策和应急处置机制，落实安全责任制，检验机构总体应急预案及各分预案的有效性，促进机构全员深入掌握应急预案，完善应急准备	目的：通过实操演练磨合机构内部应急指挥、决策和应急处置机制，检验机构总体应急预案及各分预案中各项应急操作流程的有效性、可执行性，培养机构全员的临场应变能力	目的：通过示范演练提示风险，提升机构领导层对网络安全事件应急演练的重视程度；促进机构内部应急工作交流

表 A.1（续）

演练对象	专项桌面推演	专项实操演练	专项示范演练	综合性桌面推演	综合性实操演练	综合性示范演练
组织	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单	可套用模板： B.2 应急演练工作方案 B.5 应急演练脚本 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单	可套用模板： B.2 应急演练工作方案 B.5 应急演练脚本 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单
行业	适用范围：适用于根据行业年度演练计划，由行业监管/主管部门牵头行业各有关机构，或由行业某机构发起涉及行业其他业务关联机构的，针对某一专项应急功能设置的故障场景	适用范围：适用于根据行业年度演练计划，由行业监管/主管部门牵头行业各有关机构，或由行业某机构发起涉及行业其他业务关联机构的，针对某一专项应急功能设置的故障场景	适用范围：适用于根据行业年度演练计划，由行业监管/主管部门牵头行业各有关机构，或由行业某机构发起涉及行业其他业务关联机构的，针对某一专项应急功能设置的故障场景	适用范围：适用于根据行业年度演练计划，由行业监管/主管部门牵头行业各有关机构，或由行业某机构发起的、涉及行业其他业务关联机构的，针对可能引发行业全局性风险的事件设置的综合性场景	适用范围：适用于根据行业年度演练计划，由行业监管/主管部门牵头行业各有关机构，或由行业某机构发起的、涉及行业其他业务关联机构的，针对可能引发行业全局性风险的事件设置的综合性场景	适用范围：适用于根据行业年度演练计划，由行业监管/主管部门牵头行业各有关机构，或由行业某机构发起的、涉及行业其他业务关联机构的，针对可能引发行业全局性风险的事件设置的综合性场景
	目的：通过桌面推演提高行业总体应急指挥决策协调力，检验行业专项预案及各级机构有关专项应急预案有效性，促进相关人员深入掌握应急预案，完善应急准备	目的：通过实操演练提高行业总体应急指挥决策协调力，检验行业专项预案流程及各级机构有关专项应急预案中各项应急操作流程的有效性、可执行性，培养有关人员的临场应变能力	目的：通过示范演练提示风险，切实提升行业各机构领导层对网络安全事件应急演练的重视程度；促进行业机构之间应急工作交流	目的：通过桌面推演提高行业总体应急指挥决策协调力，梳理行业各业务条线上下游机构间的耦合关系，完善各机构间应急响应联动策略，落实安全责任制，检验行业总体预案及各级机构有关专项应急预案有效性，促进相关人员掌握应急预案，完善应急准备	目的：通过实操演练提高行业总体指挥决策协调力，磨合行业内各机构之间应急响应联动机制，检验行业总体预案流程及各级机构有关专项应急预案中各项应急操作流程的有效性、可执行性，培养有关人员的临场应变能力	目的：通过示范演练提示风险，切实提升行业各机构领导层对网络安全事件应急演练的重视程度；促进行业机构之间应急工作交流

表 A.1（续）

演练对象	专项桌面推演	专项实操演练	专项示范演练	综合性桌面推演	综合性实操演练	综合性示范演练
行业	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单	可套用模板： B.2 应急演练工作方案 B.5 应急演练脚本 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单	可套用模板： B.2 应急演练工作方案 B.5 应急演练脚本 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单
跨行业	适用范围：适用于由某一行业发起的、涉及其他行业或有关业务关联机构的，针对某一专项应对功能设置的故障场景	适用范围：适用于由某一行业发起的、涉及其他行业或有关业务关联机构的，针对某一专项应对功能设置的故障场景	适用范围：适用于由某一行业发起的、涉及其他行业或有关业务关联机构的，针对某一专项应对功能设置的故障场景	适用范围：适用于由某一行业发起的、涉及其他行业或有关业务关联机构的，可能引发多行业安全风险的事件设置的综合性场景	适用范围：适用于由某一行业发起的、涉及其他行业或有关业务关联机构的，可能引发多行业安全风险的事件设置的综合性场景	适用范围：适用于由某一行业发起的、涉及其他行业或有关业务关联机构的，可能引发多行业安全风险的事件设置的综合性场景
	目的：通过桌面推演提高跨行业应急指挥协调能力，梳理各行业之间的应急联动关系，完善行业间应急响应联动机制，检验各行业有关专项应急预案有效性，促进相关人员深入掌握应急预案，完善应急准备	目的：通过实操演练提高跨行业应急指挥协调能力，磨合行业间应急响应联动策略，检验各行业有关专项应急预案中各项应急操作流程的有效性、可执行性，培养有关人员的临场应变能力	目的：通过示范演练提示风险，切实提升行业各机构领导层对网络安全事件应急演练的重视程度；促进行业之间应急工作交流	目的：通过桌面推演提高跨行业应急指挥协调能力，梳理各行业之间的应急联动关系，完善行业间应急响应联动机制，检验各行业总体应急预案及有关分预案的有效性，促进相关人员深入掌握应急预案，完善应急准备	目的：通过实操演练提高跨行业应急指挥协调能力，磨合行业间应急响应联动策略，检验各行业总体应急预案及有关分预案中各项应急操作流程的有效性、可执行性，培养有关人员的临场应变能力	目的：通过示范演练提示风险，切实提升行业各机构领导层对网络安全事件应急演练的重视程度；促进行业之间应急工作交流

表 A.1（续）

演练对象	专项桌面推演	专项实操演练	专项示范演练	综合性桌面推演	综合性实操演练	综合性示范演练
跨行业	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单	可套用模板： B.2 应急演练工作方案 B.5 应急演练脚本 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单	可套用模板： B.2 应急演练工作方案 B.5 应急演练脚本 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单
地区				适用范围：适用于由某一地区（省市县级单位）发起的、针对可能对局部地区造成影响的事件设置的故障场景。主要为自然灾害或突发公共事件	适用范围：适用于由某一地区（省市县级单位）发起的、针对可能对局部地区造成影响的事件设置的故障场景。主要为自然灾害或突发公共事件	适用范围：适用于由某一地区（省市县级单位）发起的、针对可能对局部地区造成影响的事件设置的故障场景。主要为自然灾害或突发公共事件
				目的：通过桌面推演提高地区性应急组织机构的指挥协调能力，梳理各关联地区及有关行业应急响应联动机制，检验各地区、行业总体应急预案及有关分预案的有效性，促进相关人员深入掌握应急预案，完善应急准备	目的：通过实操演练提高地区性应急组织机构应急指挥和协调能力，磨合各关联地区及有关行业应急联动处置策略，检验地区、行业总体应急预案及有关分预案中各项应急操作流程的有效性、可执行性，培养有关人员的临场应变能力	目的：通过示范演练提升地区性应急组织机构及有关行业网络安全事件应对能力，强化安全意识宣贯；促进地区之间应急工作交流

表 A.1（续）

演练对象	专项桌面推演	专项实操演练	专项示范演练	综合性桌面推演	综合性实操演练	综合性示范演练
地区				可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单	可套用模板： B.2 应急演练工作方案 B.5 应急演练脚本 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单
跨地域				适用范围：适用于由某一地区（省/市/县级单位）发起的、针对可能造成跨地域影响的事件设置的故障场景。主要为自然灾害或突发公共事件	适用范围：适用于由某一地区（省/市/县级单位）发起的、针对可能造成跨地域影响的事件设置的故障场景。主要为自然灾害或突发公共事件	适用范围：适用于由某一地区（省/市/县级单位）发起的、针对可能造成跨地域影响的事件设置的故障场景。主要为自然灾害或突发公共事件
				目的：通过桌面推演提高跨地域性应急组织机构的指挥协调能力，梳理各关联地区及有关行业应急响应联动机制，检验各地区、行业总体应急预案及有关分预案的有效性，促进相关人员深入掌握应急预案，完善应急准备	目的：通过实操演练提高跨地域性应急组织机构应急指挥和协调能力，磨合各关联地区及有关行业应急联动处置策略，检验地区、行业总体应急预案及有关分预案中各项应急操作流程的有效性、可执行性，培养有关人员的临场应变能力	目的：通过示范演练提升跨地域性应急组织机构及有关行业网络安全事件应对能力，强化安全意识宣贯；促进地区之间应急工作交流

表 A.1（续）

演练对象	专项桌面推演	专项实操演练	专项示范演练	综合性桌面推演	综合性实操演练	综合性示范演练
跨地域				可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告	可套用模板： B.2 应急演练工作方案 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单	可套用模板： B.2 应急演练工作方案 B.5 应急演练脚本 B.7 应急演练记录单 B.8 应急演练评估单 B.9 应急演练总结报告 B.6 事件报告单

附 录 B
（资料性附录）
应急演练各步骤参考模板

B.1 应急演练计划

应急演练计划模板见表 B.1。

表 B.1 应急演练计划

序号	演练项目	目的/要求	演练方式	演练时间	参演机构或部门	演练过程安排	经费是否纳入预算（是/否）

注 1：目的/要求：明确开展应急演练的原因、要解决的问题和期望达到的效果（在对事先设定事件场景风险和应急预案认真分析的基础上，结合年度内发生网络安全事件的情况，分析和查找薄弱环节，确定需调整的演练人员、需锻炼的技能、需检验的设备、需完善的应急处置流程和需进一步明确的职责）。

注 2：演练方式：桌面推演/实操演练/示范演练，跨行业/跨地区/单位内部/部门内部，综合演练/专项演练。

注 3：演练时间：建议党政机关、企事业单位及社会团体每年组织一次综合演练，不定期组织专项演练或小范围演练。

注 4：演练过程安排：包括但不限于预案评审、演练通知、演练环境部署、执行演练方案、演练报告编写、更新预案等环节。

注 5：建议每年 12 月前完成下一年度的演练计划，并将有关经费纳入预算。

B.2 应急演练工作方案

应急演练工作方案模板见表 B.2。

表 B.2　应急演练工作方案

<table>
<tr><td colspan="5">演练概要</td></tr>
<tr><td>演练时间</td><td colspan="2"></td><td>演练地点</td><td></td></tr>
<tr><td>演练目的</td><td colspan="4"></td></tr>
<tr><td>场景设置</td><td colspan="4"></td></tr>
<tr><td>演练形式</td><td colspan="2">□桌面推演　□实操演练　□示范演练</td><td colspan="2">□组织内部　□行业内部　□跨行业　□地域性　□跨地区</td><td>□综合演练　□专项演练</td></tr>
<tr><td rowspan="10">参演团队构成
（单位、角色、
职责分工）</td><td colspan="2">管理部门</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td rowspan="3">指挥机构</td><td>指挥组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>策划组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>督导组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td rowspan="6">参演机构</td><td>顾问组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>实施组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>保障组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>评估组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>技术支持组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>观察组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>演练内容</td><td colspan="4">指导思想：
工作原则：
演练目的：
演练场景：
演练流程：
其他准备事项：
工作要求：
其他：</td></tr>
</table>

B.3　应急演练保障方案

应急演练保障方案模板见表 B.3。

表 B.3　应急演练保障方案

演练概要			
保障对象		保障范围	
保障需求			
保障目的			
牵头单位/部门		配合单位/部门	
演练方案	人员保障：××××		
	经费保障：		
	场地保障：		
	基础设施保障：		
	通信保障：		
	技术保障		
	安全保障：		
	保障检查：		

B.4　应急演练评估方案

应急演练评估方案模板见表 B.4。

表 B.4　应急演练评估方案

<table>
<tr><td colspan="6">演练概要</td></tr>
<tr><td colspan="2">评估时间</td><td colspan="2"></td><td>评估地点</td><td></td></tr>
<tr><td colspan="2">评估对象</td><td colspan="2"></td><td>评估形式</td><td></td></tr>
<tr><td colspan="6">评估组成员</td></tr>
<tr><td colspan="2">姓名</td><td colspan="2">单位</td><td>职务</td><td>专长领域</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="6">演练评估</td></tr>
<tr><td>序号</td><td>评估项目</td><td>评估指标</td><td colspan="2">评估结论
（1—差、3—合格、5—优秀）</td><td>改进建议</td></tr>
<tr><td>1</td><td>演练方案可行性</td><td>◆演练方案的合理性，可用性
◆演练方案与预案符合程度</td><td colspan="2"></td><td></td></tr>
<tr><td>2</td><td>监控告警能力</td><td>◆告警信息是否及时、准确</td><td colspan="2"></td><td></td></tr>
<tr><td>3</td><td>故障定位能力</td><td>◆是否准确定位故障点
◆是否及时根据预案提出解决方案</td><td colspan="2"></td><td></td></tr>
<tr><td>4</td><td>现场指挥协调能力</td><td>◆现场是否迅速建立应急指挥部
◆是否有明确的总指挥和现场指挥
◆总指挥和现场指挥命令下达是否正确
◆各主管部门是否迅速到位，每个人员标志清楚</td><td colspan="2"></td><td></td></tr>
<tr><td>5</td><td>参演人员处置能力</td><td>◆是否就位迅速，职责明确
◆是否处置及时
◆是否正确向指挥部反馈处置情况</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="3">综合评价</td><td colspan="2"></td><td></td></tr>
</table>

B.5 应急演练脚本

应急演练脚本模板见表 B.5。

表 B.5 应急演练脚本

<table>
<tr><td colspan="5">演练概要</td></tr>
<tr><td>演练时间</td><td colspan="2"></td><td>演练地点</td><td></td></tr>
<tr><td>演练目的</td><td colspan="4"></td></tr>
<tr><td>场景设置</td><td colspan="4"></td></tr>
<tr><td>演练形式</td><td colspan="2">□桌面推演 □实操演练 □示范演练</td><td colspan="2">□组织内部 □行业内部 □跨行业 □地域性 □跨地区</td><td>□综合演练 □专项演练</td></tr>
<tr><td>管理部门</td><td colspan="2"></td><td colspan="2">参演机构</td><td></td></tr>
<tr><td rowspan="10">参演团队构成
（单位、角色、
职责分工）</td><td colspan="2">管理机构</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td rowspan="3">指挥机构</td><td>指挥组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>策划组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>督导组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td rowspan="6">参演机构</td><td>顾问组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>实施组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>保障组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>评估组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>技术支持组</td><td colspan="2">××（人员）：×××××职责</td></tr>
<tr><td>观察组</td><td colspan="2">××（人员）：×××××职责</td></tr>
</table>

表 B.5（续）

<table>
<tr><td rowspan="7">演练保障</td><td colspan="9">人员保障：××××</td></tr>
<tr><td colspan="9">经费保障：××××</td></tr>
<tr><td colspan="9">场地保障：××××</td></tr>
<tr><td colspan="9">基础设施保障：××××</td></tr>
<tr><td colspan="9">通信保障：××××</td></tr>
<tr><td colspan="9">安全保障：××××</td></tr>
<tr><td colspan="9">保障检查：××××</td></tr>
<tr><td colspan="10">演练方案剧本</td></tr>
<tr><td>演练阶段</td><td>序号</td><td>演练主线
（按方案步骤执行）</td><td>场景展示
（镜头）</td><td>角色</td><td>指令/报告/应答</td><td>动作</td><td>同步场景</td><td>角色/动作</td><td>备注</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

B.6 事件报告单

事件报告单模板见表 B.6。

表 B.6　事件报告单

报告时间：　　年　　月　　日　　时　　分　　第　　次

机构名称		报告人	
联系电话		传 真	
签发人		联系方式（含手机）	
事件发生时间、地点			
事件简要经过			
事件影响范围、影响程度、影响人数、经济损失情况			
事件导致的后果、发生原因和事件性质判断			
已采取的措施及效果			
需要有关部门和单位协助处置的有关事宜			
备注			

B.7 应急演练记录单

应急演练记录单模板见表 B.7。

表 B.7 应急演练记录单

<table>
<tr><td colspan="8">演练概要</td></tr>
<tr><td>演练时间</td><td colspan="2"></td><td>演练地点</td><td colspan="4"></td></tr>
<tr><td>演练目的</td><td colspan="7"></td></tr>
<tr><td>场景设置</td><td colspan="7"></td></tr>
<tr><td>演练形式</td><td colspan="2">□桌面推演 □实操演练 □示范演练</td><td colspan="3">□跨行业 □跨地区 □机构内部 □行业内部</td><td colspan="2">□综合演练
□专项演练</td></tr>
<tr><td>管理部门</td><td colspan="2"></td><td colspan="3">参演机构</td><td colspan="2"></td></tr>
<tr><td colspan="8">演练记录</td></tr>
<tr><td>演练阶段</td><td>序号</td><td>起止时间</td><td>演练过程控制情况</td><td>参演人员表现</td><td>意外情况及其处置（选填）</td><td>记录人</td><td>记录手段</td></tr>
<tr><td>系统准备及启动</td><td>1</td><td></td><td>□系统备份等安全控制措施
□演练前是否向指挥组确认
□指挥组是否正式宣布演练开始
□其他（请补充说明）</td><td></td><td></td><td></td><td>□文字
□照片
□音像
□其他（补充说明具体手段）</td></tr>
<tr><td>演练执行</td><td>2</td><td></td><td>□演练指挥组组长是否对演练全过程进行控制或授权协调组控制
□保障组是否按照演练预案进行事件场景模拟
□参演机构是否指定专人按预案要求将发现的问题和处置情况向协调组报告
□实施组是否将演练进展情况及时向协调组报告
□演练执行过程是否做好全演练执行过程记录
□其他（请补充说明）</td><td></td><td></td><td></td><td></td></tr>
</table>

表 B.7（续）

演练阶段	序号	起止时间	演练过程控制情况	参演人员表现	意外情况及其处置（选填）	记录人	记录手段
演练结束与终止	3		□演练结束后，是否由指挥组宣布演练结束，且所有人员停止了演练活动 □各参演机构和指挥机构是否及时总结 □各参演机构和指挥机构对演练现场是否进行清理 □演练过程中出现突发相关情形，指挥组是否提前终止演练 □其他（请补充说明）				
系统恢复	4		□各参演机构是否恢复系统 □各参演机构是否向指挥组报告系统恢复情况 □演练结束后次日是否向指挥组书面报告系统运行状态 □其他（请补充说明）				

B.8 应急演练评估单

应急演练评估单模板见表 B.8。

表 B.8　应急演练评估单

演练概要				
演练时间		演练地点		
演练目的				
场景设置				
演练形式	□桌面推演　□实操演练　□示范演练	□跨行业　□跨地区　□机构内部　□行业内部		□综合演练　□专项演练
管理部门		参演机构		
评估组成员				
姓名	单位	职务		专长领域
演练评估				
序号	评估项目	评估指标	评估结论 （1—差、3—合格、5—优秀）	改进建议
1	演练方案可行性	◆演练方案的合理性，可用性 ◆演练方案与预案符合程度		
2	监控告警能力	◆告警信息是否及时、准确		
3	故障定位能力	◆是否准确定位故障点 ◆是否及时根据预案提出解决方案		
4	现场指挥协调能力	◆现场是否迅速建立应急指挥机构 ◆是否有明确的指挥组组长和协调者 ◆指挥组和协调组命令下达是否正确 ◆各主管部门是否迅速到位，每个人员标志清楚		

表 B.8（续）

序号	评估项目	评估指标	评估结论 （1—差、3—合格、5—优秀）	改进建议
5	参演人员处置能力	◆是否就位迅速，职责明确 ◆是否处置及时 ◆是否正确向指挥部反馈处置情况		
6	关联方应急联动能力	◆接口部门及人员是否明确 ◆是否响应及时 ◆配合是否流畅		
7	演练保障能力	◆应急人员（主备岗）是否及时就位 ◆技术备品备件是否充足 ◆应急物资及必要通信设备准备是否充足 ◆是否制定意外情况应急措施和回退方案		
8	演练目标的实现情况	◆是否通过演练发现待改进事项 ◆是否达到预期目标		
9	演练的成本效益分析	◆是否符合演练预算，厉行节约		

B.9 应急演练总结报告

应急演练总结报告模板见表 B.9。

表 B.9　应急演练总结报告

演练概要			
演练时间		演练地点	
演练目的			
场景设置			
演练形式	□桌面推演　□实操演练　□示范演练	□跨行业　□跨地区　□机构内部　□行业内部	□综合演练　□专项演练
牵头单位		参演机构	
演练评估			
演练评估时间		演练评估地点	
评估专家组成员			
评估结论			
演练总结及改进思路			
演练总结			
改进思路			

附　录　C
（资料性附录）
演练场景库

演练场景库见表 C.1。

表 C.1　演练场景库

常见风险类型	常见故障类型	故障场景描述	建议演练形式
自然灾害风险	太阳黑子活动	由于太阳黑子活动，导致技术系统遭受一定程度干扰，出现运行异常等情况	机构层面专项桌面推演/行业层面专项桌面推演
	台风	沿海地区受台风影响，可能出现电力中断、通信线路受损、水害等，影响系统正常运行，甚至导致系统中断 由台风导致的区域性电力、通信、交通瘫痪及社会公共安全等应急场景	机构层面综合性桌面推演/地区层面综合性桌面推演
	破坏性地震	由地震引发的地域性社会救援、医疗卫生、电力、通信、运输等应急场景	机构层面综合性桌面推演/地区层面综合性桌面推演/地区层面综合性示范演练
	水灾	因水灾引起的机房地下基础设施被淹、机房渗漏等，影响技术系统正常运行以及市政排水、社会救援、交通等应急场景	机构层面综合性桌面推演/地区层面综合性桌面推演
	火灾	机房火灾导致的技术系统不可用 火灾现场人员疏散、救援、消防等应急场景	机构层面综合性桌面推演/机构层面综合性实操演练
技术系统风险	计算机硬件故障	由于服务器硬件、网络设备、存储设备等故障导致的系统不可用	机构层面专项桌面推演/机构层面专项实操演练/行业层面综合性实操演练
	计算机软件故障	由于计算机软件逻辑错误、软件缺陷、变更失败等导致的系统不可用	机构层面专项桌面推演/机构层面专项实操演练/行业层面综合性实操演练
	机房基础设施故障	由于机房配电、通信线路、空调、消防系统等基础设施故障导致的系统不可用	机构层面专项桌面推演/机构层面专项实操演练/行业层面综合性实操演练
	系统容量不足	由于系统性能不够、处理能力不足导致的运行缓慢或业务中断等场景	机构层面专项桌面推演/机构层面专项实操演练/行业层面综合性实操演练

表 C.1（续）

常见风险类型	常见故障类型	故障场景描述	建议演练形式
工控系统风险	工业控制类设备故障	工业控制系统软硬件故障所导致的等业务中断	机构层面专项桌面推演/行业层面专项桌面推演/地区层面综合性桌面推演
	工业控制类设备受到攻击	攻击者利用工业控制系统漏洞、协议缺陷等对系统进行攻击渗透导致的系统运行异常或不可用	机构层面专项桌面推演/行业层面专项桌面推演/地区层面综合性桌面推演
	业务规则紧急调整	业务规则逻辑错误或调整后测试不充分导致的系统运行异常或不可用	机构层面专项桌面推演/行业层面专项桌面推演/地区层面综合性桌面推演
互联网安全风险	网络攻击事件	通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷造成系统异常或对信息系统运行造成潜在危害的互联网安全事件	机构层面专项实操演练/行业层面专项实操演练
	有害程序事件	蓄意制造、传播有害程序，或是因受到有害程序影响而导致的互联网安全事件	机构层面专项实操演练/行业层面专项实操演练
	信息破坏事件	通过网络或其他技术手段造成信息系统中信息被篡改、假冒、泄露、窃取而导致的互联网安全事件	机构层面专项实操演练/行业层面专项实操演练
	信息内容安全事件	利用信息网络发布、传播危害国家安全、社会稳定和公共利益内容的互联网安全事件	机构层面专项实操演练/行业层面专项实操演练/地区层面专项实操演练
其他行业关联风险	大面积电力故障	由于电力行业发电或传输系统故障导致的区域性事件或其他行业遭受连带影响的事件	机构层面综合性实操演练/行业层面综合性实操演练/地区层面综合性桌面推演/跨地域综合性桌面推演
	大面积通信故障	由于通信行业线路故障导致的区域性事件或其他行业遭受连带影响的事件	机构层面综合性实操演练/行业层面综合性实操演练/地区层面综合性桌面推演/跨地域综合性桌面推演
	其他行业故障	某行业故障导致其他关联行业遭受连带影响的事件	机构层面综合性实操演练/行业层面综合性实操演练
技术创新风险	云服务提供商故障	由于云服务商故障导致的业务中断或业务数据丢失、损毁等事件	机构层面综合性实操演练/行业层面综合性实操演练
	其他故障	其他	

附　录　D
（资料性附录）
参考案例

D.1　设备设施故障实操演练案例

设备设施故障实操演练案例适用于针对信息系统自身软硬件故障，电力、通信等外围保障设施故障，受关联单位故障影响及认为操作失误等导致网络安全事件的应急演练。本案例模拟某单位生产系统硬件故障切换备份系统运行的场景，演练期间各项活动所需表格可参照表 D.1～表 D.4。

表 D.1　设备设施故障实操演练方案

演练方案概要			
演练时间	YYYY-MM-DD	演练地点	××单位××系统所在机房/备份中心
演练目的	检验信息系统重大技术故障的发现、定位、指挥及协同处置能力，验证应急预案和应急处置流程，检验备份/灾备系统建设能及和可用性，锻炼团队		
场景设置	××单位生产时间××系统突发技术故障，导致系统不可用，有关业务中断。经判断为主用生产系统硬件故障，随即启动应急预案，将生产系统向备份系统切换，同时有关部门组织发布信息，开展舆论引导		
演练形式	□桌面推演　■实操演练　□示范演练	□跨行业　□跨地区　■单位内部　□部门内部	□综合演练　■专项演练
管理单位	××单位系统运行部	参演机构	××单位综合部、有关业务部
参演团队构成（单位、角色、职责分工）	指挥组：技术部门分管领导、运行部负责人、综合部负责人、有关业务部门负责人 策划组：系统运行部负责编写方案、组织策划 保障组：系统运行部（运行一线、二线人员）负责安全保障（明确到人） 评估组：系统运行部、综合部、有关业务部门派员组成评估小组		
演练保障	人员保障：演练各项工作落实到人（安排主备岗），演练准备及实施全程参与（明确到人） 经费保障：按照年度演练计划和预算落实 物资保障：技术系统备品备件等…… 场地保障：演练所在机房，灾备中心 通信保障：专线等通信链路，固定电话、手机等必要联络设备		

表 D.1（续）

演练方案							
演练阶段	序号	时间控制	演练步骤	动作	角色 （执行方）	同步执行	角色/动作
演练开始	1	T	向演练现场下达演练开始指令				
	2	T+1	模拟××系统生产主机硬件故障	（停止服务进程等方式）			
发现故障并记录	3	T+2	一线运行监控人员通过统一监控系统发现报警信息，向二线运管中心报告故障	查看监控界面	一线运行监控	与此同时，业务部门陆续接到下级单位报障电话，反映××业务出现中断	业务部门
	4	T+3	二线运管中心接到报告，对故障进行定位，经判断，××系统为生产主机硬件故障	组织进行故障研判	二线运管中心		
	5	T+4	按照预案，应立即将生产系统向备份系统切换，运管中心人员向运行负责任报告故障情况，建议立即启动预案	向运行负责人报告	二线运管中心		
	6	T+5	运行负责人同意启动预案		运行负责人		
预案启动	7	T+6	二线运管中心通知××系统管理员准备进行系统切换		二线运管中心××系统管理员		
	8	T+6	通知有关业务部门进行制定统一解释口径，通过短信、网站公告、客户电话等形式提示风险，开展舆情监控。		业务部门		
	9	T+6	通知综合部门编制《网络安全事件报告书》向有关部门报告情况。		综合部门		
	10	T+6	通知有关硬件厂商携带备件赶赴故障现场进行处置	致电硬件厂商			
	11	T+7	××系统管理员将生产系统向备份系统切换，切换完成后持续关注数据同步情况，通知一线运行监控关注下级单位链接情况	系统切换、数据同步	××系统管理员		

表 D.1（续）

演练阶段	序号	时间控制	演练步骤	动作	角色 （执行方）	同步执行	角色/动作
系统恢复	12	T+16	确定数据同步完成，各方链接正常，二线运管中心向运行负责人报告系统恢复情况，告知厂商已赶到现场对故障硬件进行更换，并建议在本阶段生产运行结束后切换回主用生产系统	向运行负责人报告切换情况	二线运管中心		
	13	T+19	通知业务部门通过网站等形式发布公告通知业务恢复正常，通知综合部门向有关单位报告恢复情况		二线运管中心		
演练完成	14	T+20	宣布演练结束				

表 D.2　设备设施故障实操演练记录单

演练概要			
演练时间	YYYY-MM-DD	演练地点	××单位××系统所在机房/备份中心
演练目的	检验信息系统重大技术故障的发现、定位、指挥及协同处置能力，验证应急预案和应急处置流程，检验备份/灾备系统建设能及和可用性，锻炼团队		
场景设置	××单位生产时间××系统突发技术故障，导致系统不可用，有关业务中断。经判断为主用生产系统硬件故障，随即启动应急预案，将生产系统向备份系统切换，同时有关部门组织发布信息，开展舆论引导		
演练形式	□桌面推演　■实操演练　□示范演练	□跨行业　□跨地区　■单位内部　□部门内部	□综合演练　■专项演练
管理部门	××单位系统运行部	参演机构	××单位综合部、有关业务部

表 D.2（续）

演练记录							
演练阶段	序号	起止时间	演练过程控制情况	参演人员表现	意外情况及其处置(选填)	记录人	记录手段
系统准备及启动	1	YYYY-MM-DD 9:00-9:02	■系统备份等安全控制措施 ■演练前是否向总指挥部确认 ■总指挥部是否正式宣布演练开始 □其他(请补充说明)	良好	无	× ××	■文字 □照片 □音像 □其他(补充说明具体手段)
演练执行	2	YYYY-MM-DD 9:03-9:15	■演练总指挥是否对演练全过程进行控制或授权策划组控制 ■各应急指挥中心是否按照演练预案进行事件场景模拟 ■演练单位是否指定专人按预案要求将发现的问题和处置情况向总指挥部报告 ■各应急指挥中心领导小组是否将演练进展情况及时向总指挥报告 ■演练执行过程是否做好全演练执行过程记录 □其他(请补充说明)	良好	无	× ××	■文字 □照片 □音像 □其他(补充说明具体手段)
演练结束与终止	3	YYYY-MM-DD 9:16-9:20	■演练结束后,是否由总指挥部宣布演练结束,且所有人员停止了演练活动 ■各应急指挥中心和总指挥部是否及时总结 ■各应急指挥中心和总指挥部对演练现场是否进行清理 □演练过程中出现突发相关情形,总指挥部领导小组是否提前终止演练 □其他(请补充说明)	良好	无	× ××	■文字 □照片 □音像 □其他(补充说明具体手段)
系统恢复	4	YYYY-MM-DD 9:30 之后	■各参演机构是否恢复系统 ■各参演机构是否向总指挥部报告系统恢复情况 ■演练结束后次日是否向总指挥部书面报告系统运行状态 □其他(请补充说明)	良好	无	× ××	■文字 □照片 □音像 □其他(补充说明具体手段)

表 D.3　设备设施故障实操演练评估

演练概要					
演练时间	YYYY-MM-DD		演练地点	××单位××系统所在机房/备份中心	
演练目的	检验信息系统重大技术故障的发现、定位、指挥及协同处置能力，验证应急预案和应急处置流程，检验备份/灾备系统建设能及和可用性，锻炼团队				
场景设置	××单位生产时间××系统突发技术故障，导致系统不可用，有关业务中断。经判断为主用生产系统硬件故障，随即启动应急预案，将生产系统向备份系统切换，同时有关部门组织发布信息，开展舆论引导				
演练形式	□桌面推演　■实操演练　□示范演练		□跨行业　□跨地区　■单位内部　□部门内部		□综合演练　■专项演练
管理部门	××单位系统运行部		参演机构	××单位综合部、有关业务部	
评估组成员					
姓名	单位		职务	专长领域	
×××	××单位系统运行部		总监	……	
×××	××单位××业务部		总监	……	
……	……		……	……	
演练评估					
序号	评估项目	评估指标	评估结论 （1—差、3—合格、5—优秀）	改进建议	
1	演练方案可行性	◆演练方案的合理性，可用性 ◆演练方案与预案符合程度	演练方案合理，与预案基本符合，得分：3	建议根据演练情况进一步修订完善预案	
2	监控告警能力	◆告警信息是否及时、准确	及时、准确，得分：5		
3	故障定位能力	◆是否准确定位故障点 ◆是否及时根据预案提出解决方案	能够根据告警信息及时定位故障点并按照预案确定处置方案，得分：3	建议持续丰富和细化预案场景库	

表 D.3（续）

序号	评估项目	评估指标	评估结论 （1—差、3—合格、5—优秀）	改进建议
4	现场指挥协调能力	◆现场是否迅速建立应急指挥部 ◆是否有明确的总指挥和现场指挥 ◆总指挥和现场指挥命令下达是否正确 ◆各主管部门是否迅速到位，每个人员标志清楚	组织架构明确，各方响应迅速，得分：5	
5	参演人员处置能力	◆是否就位迅速，职责明确 ◆是否处置及时 ◆是否正确向指挥部反馈处置情况	应急过程中各方职责分工清晰，处置迅速且及时向指挥部反馈处置进展，得分：5	
6	关联方应急联动能力	◆接口部门及人员是否明确 ◆是否响应及时 ◆配合是否流畅	与关联方对接顺利，各关联方配合及时准确，得分：5	
7	演练保障能力	◆应急人员（主备岗）是否及时就位 ◆技术备品备件是否充足 ◆应急物资及必要通信设备准备是否充足 ◆是否制定意外情况应急措施和回退方案	制定了紧急情况回退方案，应急人员、设备、物资等充足，得分：5	
8	演练目标的实现情况	◆是否通过演练发现待改进事项 ◆是否达到预期目标	已针对需要改进事项提出有关建议，经评估，演练达到预期目标，得分：5	
9	演练的成本效益分析	◆是否符合演练预算，厉行节约	严格按照预算开展演练，得分：5	

表 D.4　设备设施故障实操演练总结

演练概要			
演练时间	YYYY-MM-DD	演练地点	××单位××系统所在机房/备份中心
演练目的	检验信息系统重大技术故障的发现、定位、指挥及协同处置能力，验证应急预案和应急处置流程，检验备份/灾备系统建设能及和可用性，锻炼团队		
场景设置	××单位生产时间××系统突发技术故障，导致系统不可用，有关业务中断。经判断为主用生产系统硬件故障，随即启动应急预案，将生产系统向备份系统切换，同时有关部门组织发布信息，开展舆论引导		
演练形式	□桌面推演　■实操演练　□示范演练	□跨行业　□跨地区　■单位内部　□部门内部	□综合演练　■专项演练
管理部门	××单位系统运行部	参演机构	××单位综合部、有关业务部
演练评估			
演练评估时间	YYYY-MM-DD	演练评估地点	××单位会议室
评估专家组成员	技术、综合及有关部门负责人		
评估结论	演练方案涉及合理，与预案基本符合； 告警及时、准确，能够根据告警信息及时定位故障点并按照预案确定处置方案； 组织架构明确，各方响应迅速，职责分工清晰，处置迅速； 与关联方对接顺利，各关联方配合及时有效； 达到预期演练目标		
演练总结及改进思路			
演练总结	将于演练结束两周内编制详细演练总结及整改方案		
改进思路	将于演练结束两周内编制详细演练总结及整改方案		

D.2 灾害性事件桌面推演案例

灾害性事件桌面推演方案适用于针对台风、暴雨、洪水、火灾、地震、大面积停电、恐怖袭击、战争等不可抗力所引发网络安全事件的应急演练，演练期间各项活动所需表格可参照表D.5～表D.8。该案例模拟某单位大楼火灾引发停电影响技术系统运行的场景。

表D.5 灾害性事件桌面推演方案

演练方案概要			
演练时间	YYYY-MM-DD	演练地点	××单位数据中心
演练目的	检验单位各部门针对火灾类突发事件的应对能力及灾备系统可用性，完善与各关联单位的应急响应联动机制，提高全体人员消防安全意识与应变自救能力		
场景设置	模拟××单位数据中心所在大楼突发火灾，消防部门接到报警抵达现场并准备对大楼进行封锁，××单位配合消防部门对大楼人员进行紧急疏散，同时启动应急预案，紧急将重要技术系统切换至灾备中心，技术人员撤离		
演练形式	■桌面推演 □实操演练 □示范演练	■跨行业 □跨地区 □单位内部 □部门内部	■综合演练 □专项演练
管理部门	××单位运维部门	参演机构	大楼物业、消防部门
参演团队构成（单位、角色、职责分工）	指挥组：××单位总经理、单位所有部门负责人组成指挥组（分指挥部），总经理任（分指挥部）指挥（明确到人） 策划组：运维部门牵头，会同各参演部门有关人员组成策划组，开展演练方案制定、剧本编写等（明确到人） 保障组：运维部会同大楼物业负责演练过程中的安全保障（明确到人，以及联系方式） 观察组：有关部门领导出席演练，进行观察指导 评估组：行业有关信息技术专家组成评估小组对演练情况开展评估（明确到人）		
演练保障	人员保障：演练各项工作落实到人（安排主备岗），演练准备及实施全程参与（明确到人） 经费保障：按照××年度演练计划和预算落实 物资保障：技术系统备品备件、消防设施（呼吸器等）、紧急照明设施…… 场地保障：演练所在大楼及周边区域，灾备中心 通信保障：专线等通信链路，固定电话、手机、对讲机等必要联络设备		

表 D.5（续）

演练方案							
演练阶段	序号	时间控制	演练步骤	动作	角色 （执行方）	同步执行	角色/动作
演练开始	1	T	向××单位下达演练开始指令		总指挥部		
	2	T+1	××单位接受指令，介绍参演场景及演练内容		××单位分指挥部		
	3	T+3	××单位向演练现场下达演练开始指令		××单位分指挥部		
故障发现	4	T+4	模拟数据中心所在大楼发生火灾（通过向烟雾探测器送等方式）		××单位运维保障部门		
	5	T+5	监控人员发现消防系统出现声光报警，通过监控确认告警区域，立即赶往该区域实地查看	通过监控确认告警区域，立即赶往该区域实地查看	××单位运维监控部门		
	6	T+6	实地查看确认出现大量烟雾，暂未见明火，立即与大楼物业联系，被告知为大楼管井失火，物业已报警并将立即启动火灾应急		××单位运维监控部门	与此同时物业部门电话向消防部门报警，大楼响起火灾警报	大楼物业
						接到火灾报警，立即派出消防车赶往火灾地点	消防部门
	7	T+7	××单位运维监控人员立即向部门负责人报告情况，根据单位应急预案，已达到火灾应急预案启动条件，要求立即启动应急		××单位运维监控部门	运维负责人同意启动预案	运维负责人
预案启动	8	T+8	运维监控人员立即通知有关部门启动预案	1） 通知综合部门立即组织疏散 2） 通知系统管理员执行系统切换 3） 立即对机房内人员进行疏散，模拟启动消防系统气体释放		运维负责人紧急向单位领导报告情况，并要求按照预案服从综合部门安排立即疏散	

表 D.5（续）

演练阶段	序号	时间控制	演练步骤	动作	角色 （执行方）	同步执行	角色/动作
预案启动	9	T+10	综合部门立即派出人员分头到各办公区域组织疏散，要求全体人员切断办公设备电源马上撤离		综合部门	此时消防车抵达	综合部门与消防部门配合
	10	T+15	系统管理员按照预案要求立即将重要技术系统向灾备系统切换，同时向灾备中心运行人员告知情况，请求配合，完成指定操作并撤离		系统管理员	灾备中心对有关系统进行接管，与此同时指定专人统计影响情况并草拟《网络安全事件报告书》向上级部门报告	灾备中心
						指定人员制定统一解释口径，通过短信、网站公告、客户电话等形式提示风险，开展舆情监控，对失实报道的情况要求删除或澄清	灾备中心
	11	T+25	灾备切换完成，检查重要系统运行情况，持续向××单位指挥部（已撤离大楼）报告各交易系统切换情况		灾备中心		
恢复正常	12	T+34	模拟大楼火势已被控制，灾备系统运行正常，持续统计确认受影响范围，向上级部门报告		灾备中心	有关人员赶往灾备中心临时办公场地	
	13	T+35	报告演练完成		××单位分指挥部		

表 D.6　灾害性事件桌面推演记录单

<table>
<tr><td colspan="8">演练概要</td></tr>
<tr><td>演练时间</td><td colspan="2">YYYY-MM-DD</td><td>演练地点</td><td colspan="4">××单位数据中心</td></tr>
<tr><td>演练目的</td><td colspan="7">检验单位各部门针对火灾类突发事件的应对能力及灾备系统可用性，完善与各关联单位的应急响应联动机制，提高全体人员消防安全意识与应变自救能力</td></tr>
<tr><td>场景设置</td><td colspan="7">模拟××单位数据中心所在大楼突发火灾，消防部门接到报警抵达现场并准备对大楼进行封锁，××单位配合消防部门对大楼人员进行紧急疏散，同时启动应急预案，紧急将重要技术系统切换至灾备中心，技术人员撤离</td></tr>
<tr><td>演练形式</td><td colspan="2">■桌面推演　□实操演练　□示范演练</td><td colspan="3">■跨行业　□跨地区　□单位内部　□部门内部</td><td colspan="2">■综合演练　□专项演练</td></tr>
<tr><td>管理部门</td><td colspan="2">××单位</td><td>参演机构</td><td colspan="4">大楼物业、消防部门</td></tr>
<tr><td colspan="8">演练记录</td></tr>
<tr><td>演练阶段</td><td>序号</td><td>起止时间</td><td colspan="2">演练过程控制情况</td><td>参演人员表现</td><td>意外情况及其处置(选填)</td><td>记录人</td><td>记录手段</td></tr>
<tr><td>系统准备及启动</td><td>1</td><td>YYYY-MM-DD
9:00-9:03</td><td colspan="2">■系统备份等安全控制措施
■演练前是否向总指挥部确认
■总指挥部是否正式宣布演练开始
□其他(请补充说明)</td><td>良好</td><td>无</td><td>×××</td><td>■文字
□照片
□音像
□其他(补充说明具体手段)</td></tr>
<tr><td>演练执行</td><td>2</td><td>YYYY-MM-DD
9:04-9:30</td><td colspan="2">■演练总指挥是否对演练全过程进行控制或授权策划组控制
■各应急指挥中心是否按照演练预案进行事件场景模拟
■演练单位是否指定专人按预案要求将发现的问题和处置情况向总指挥部报告
■各应急指挥中心领导小组是否将演练进展情况及时向总指挥报告
■演练执行过程是否做好全演练执行过程记录
□其他(请补充说明)</td><td>良好</td><td>无</td><td>×××</td><td>■文字
□照片
□音像
□其他(补充说明具体手段)</td></tr>
</table>

表 D.6（续）

演练阶段	序号	起止时间	演练过程控制情况	参演人员表现	意外情况及其处置(选填)	记录人	记录手段
演练结束与终止	3	YYYY-MM-DD 9:31-9:35	■演练结束后，是否由总指挥部宣布演练结束，且所有人员停止了演练活动 ■各应急指挥中心和总指挥部是否及时总结 ■各应急指挥中心和总指挥部对演练现场是否进行清理 □演练过程中出现突发相关情形，总指挥部领导小组是否提前终止演练 □其他(请补充说明)	良好	无	×××	■文字 □照片 □音像 □其他(补充说明具体手段)
系统恢复	4	YYYY-MM-DD 9:35 之后	■各参演机构是否恢复系统 ■各参演机构是否向总指挥部报告系统恢复情况 ■演练结束后次日是否向总指挥部书面报告系统运行状态 □其他(请补充说明)	良好	无	×××	■文字 □照片 □音像 □其他(补充说明具体手段)

表 D.7　灾害性事件桌面推演评估

<table>
<tr><td colspan="5">演练概要</td></tr>
<tr><td>演练时间</td><td colspan="2">YYYY-MM-DD</td><td>演练地点</td><td>××单位数据中心</td></tr>
<tr><td>演练目的</td><td colspan="4">检验单位各部门针对火灾类突发事件的应对能力及灾备系统可用性，完善与各关联单位的应急响应联动机制，提高全体人员消防安全意识与应变自救能力</td></tr>
<tr><td>场景设置</td><td colspan="4">模拟××单位数据中心所在大楼突发火灾，消防部门接到报警抵达现场并准备对大楼进行封锁，××单位配合消防部门对大楼人员进行紧急疏散，同时启动应急预案，紧急将重要技术系统切换至灾备中心，技术人员撤离</td></tr>
<tr><td>演练形式</td><td>■桌面推演　□实操演练　□示范演练</td><td colspan="2">■跨行业　□跨地区　□单位内部　□部门内部</td><td>■综合演练　□专项演练</td></tr>
<tr><td>管理部门</td><td colspan="2">××单位</td><td>参演机构</td><td>大楼物业、消防部门</td></tr>
<tr><td colspan="5">评估组成员</td></tr>
<tr><td>姓名</td><td colspan="2">单位</td><td>职务</td><td>专长领域</td></tr>
<tr><td>×××</td><td colspan="2">××单位技术部</td><td>部门负责人</td><td>……</td></tr>
<tr><td>×××</td><td colspan="2">××单位综合部</td><td>部门负责人</td><td>……</td></tr>
<tr><td>×××</td><td colspan="2">大厦物业保障部</td><td>部门负责人</td><td>……</td></tr>
<tr><td>×××</td><td colspan="2">××区消防支队</td><td>负责人</td><td>……</td></tr>
<tr><td>……</td><td colspan="2">……</td><td>……</td><td>……</td></tr>
<tr><td colspan="5">演练评估</td></tr>
<tr><td>序号</td><td>评估项目</td><td>评估指标</td><td>评估结论
（1—差、3—合格、5—优秀）</td><td>改进建议</td></tr>
<tr><td>1</td><td>演练方案可行性</td><td>◆演练方案的合理性，可用性
◆演练方案与预案符合程度</td><td>演练方案合理，与预案基本符合，得分：3</td><td>建议根据演练情况进一步修订完善预案</td></tr>
<tr><td>2</td><td>监控告警能力</td><td>◆告警信息是否及时、准确</td><td>及时、准确，得分：5</td><td></td></tr>
<tr><td>3</td><td>故障定位能力</td><td>◆是否准确定位故障点
◆是否及时根据预案提出解决方案</td><td>能够根据告警信息及时定位故障点并按照预案确定处置方案，得分：3</td><td>建议持续丰富和细化预案场景库</td></tr>
</table>

表 D.7（续）

序号	评估项目	评估指标	评估结论 （1—差、3—合格、5—优秀）	改进建议
4	现场指挥协调能力	◆现场是否迅速建立应急指挥部 ◆是否有明确的总指挥和现场指挥 ◆总指挥和现场指挥命令下达是否正确 ◆各主管部门是否迅速到位，每个人员标志清楚	组织架构明确，各方响应迅速，得分：5	
5	参演人员处置能力	◆是否就位迅速，职责明确 ◆是否处置及时 ◆是否正确向指挥部反馈处置情况	应急过程中各方职责分工清晰，处置迅速且及时向指挥部反馈处置进展，得分：5	
6	关联方应急联动能力	◆接口部门及人员是否明确 ◆是否响应及时 ◆配合是否流畅	与关联方对接顺利，各关联方配合及时准确，得分：3	持续完善关联单位之间联络机制
7	演练保障能力	◆应急人员（主备岗）是否及时就位 ◆技术备品备件是否充足 ◆应急物资及必要通信设备准备是否充足 ◆是否制定意外情况应急措施和回退方案	制定了紧急情况回退方案，应急人员、设备、物资等充足，得分：5	
8	演练目标的实现情况	◆是否通过演练发现待改进事项 ◆是否达到预期目标	已针对需要改进事项提出有关建议，经评估，演练达到预期目标，得分：5	
9	演练的成本效益分析	◆是否符合演练预算，厉行节约	严格按照预算开展演练，得分：5	

表 D.8　灾害性事件桌面推演总结

演练概要			
演练时间	YYYY-MM-DD	演练地点	××单位数据中心
演练目的	检验单位各部门针对火灾类突发事件的应对能力及灾备系统可用性，完善与各关联单位的应急响应联动机制，提高全体人员消防安全意识与应变自救能力		
场景设置	模拟××单位数据中心所在大楼突发火灾，消防部门接到报警抵达现场并准备对大楼进行封锁，××单位配合消防部门对大楼人员进行紧急疏散，同时启动应急预案，紧急将重要技术系统切换至灾备中心，技术人员撤离		
演练形式	■桌面推演　□实操演练　□示范演练	■跨行业　□跨地区　□单位内部　□部门内部	■综合演练　□专项演练
管理部门	××单位	参演机构	大楼物业、消防部门
演练评估			
演练评估时间	YYYY-MM-DD	演练评估地点	××单位会议室
评估专家组成员	由××单位技术部、综合部及有关业务部门，大厦物业保障部，消防支队负责人等组成		
评估结论	演练方案涉及合理，与预案基本符合； 告警及时、准确，能够根据告警信息及时定位故障点并按照预案确定处置方案； 组织架构明确，各方响应迅速，职责分工清晰，处置迅速； 与关联方对接顺利，各关联方配合及时有效； 达到预期演练目标		
演练总结及改进思路			
演练总结	将于演练结束两周内编制详细演练总结及整改方案		
改进思路	将于演练结束两周内编制详细演练总结及整改方案		

D.3　网络攻击事件示范演练案例

网络攻击事件示范演练方案适用于通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷造成系统异常或对信息系统运行造成潜在危害的网络安全事件的应急演练。本样例模拟某单位门户网站遭遇 DDoS 攻击的场景，演练期间各项活动所需表格可参照表 D.9～表 D.13。

表 D.9　网络攻击事件示范演练方案

<table>
<tr><td colspan="8">演练方案概要</td></tr>
<tr><td>演练时间</td><td colspan="2">YYYY-MM-DD</td><td>演练地点</td><td colspan="4">××单位网站系统所在机房</td></tr>
<tr><td>演练目的</td><td colspan="7">检验××单位互联网安全防护能力，验证应急预案和应急处置流程，完善与各关联单位的应急响应联动机制</td></tr>
<tr><td>场景设置</td><td colspan="7">某工作日，××单位发现门户网站访问缓慢，经判断为遭遇 DDoS 攻击，紧急启动应急预案并协调网络运营商开展应急处置</td></tr>
<tr><td>演练形式</td><td colspan="2">□桌面推演　□实操演练　■示范演练</td><td colspan="3">■跨行业　□跨地区　□单位内部　□部门内部</td><td colspan="2">□综合演练　■专项演练</td></tr>
<tr><td>管理部门</td><td colspan="2">××单位技术部</td><td>参演机构</td><td colspan="4">网络运营商、CNCERT、安全厂商</td></tr>
<tr><td>参演团队构成
（单位、角色、
职责分工）</td><td colspan="7">指挥组：技术部门分管领导、技术部负责人、综合部负责人
策划组：技术部负责编写方案、组织策划
保障组：技术部负责安全保障（明确到人）
观察组：行业所有单位、有关外联单位
评估组：技术部、综合部、行业信息安全专家组成评估小组</td></tr>
<tr><td>演练保障</td><td colspan="7">技术保障：演练相关网络设备数量、型号，拟使用的监控及处置相关工具。如入侵检测系统、防火墙系统、防病毒系统等
人员保障：信息安全运维人员及演练有关技术人员全员到岗
经费保障：应急演练预算
场地保障：故障模拟场地、应急指挥场地、应急处置场地等
通信保障：热线、视频会议系统、电话会议系统、其他通信设施等</td></tr>
<tr><td colspan="8">演练方案</td></tr>
<tr><td>演练阶段</td><td>序号</td><td>时间控制</td><td>演练步骤</td><td>动作</td><td>角色
（执行方）</td><td>同步执行</td><td>角色/动作</td></tr>
<tr><td rowspan="2">演练开始</td><td>1</td><td>T</td><td>××单位向演练现场下达演练开始指令</td><td></td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>T+1</td><td>网络运营商向演练单位发起故障</td><td>中断通信线路</td><td></td><td></td><td></td></tr>
</table>

表 D.9（续）

演练阶段	序号	时间控制	演练步骤	动作	角色 （执行方）	同步执行	角色/动作
故障预警、响应及报告流程	3	T+3	××单位运维部门监控出现门户网站流量告警，运维人员对告警进行初步分析，判断为门户网站遭遇 DDoS 攻击	查看监控告警界面			
	4	T+5	监控人员向运维负责人报告故障	电话报告故障			
应急决策、指挥、处置、报告、信息发布	5	T+6	运维负责人召集应急工作小组，进一步确认故障及影响范围，研判风险，并确定启动相应应急预案	组织进行故障及风险研判			
	6	T+10	按应急预案，紧急与运营商沟通启动流量清洗服务			综合部门开展舆情监控，通过微信公众号等方式发布公告	
	7					通知网络安全厂商紧急赶来故障现场开展技术支持	
应急决策、指挥、处置、报告、信息发布	8	T+20	运营商流量清洗完成，网络流量恢复正常，门户网站恢复访问				
	9	T+25	持续跟踪门户网站运行情况，并向运维负责人报告情况	电话报告处置情况及后续工作		网络安全厂商对门户网站安全情况进行评估并提出加固方案	
	10	T+30	与 CNCERT 沟通请求提供网络攻击溯源服务	电话沟通情况，请求支援			
应急演练完毕及报告	11	T+31	对事件发生和应急处置概况等进行总结				
	12	T+35	专家点评，宣布演练结束				

表 D.10　网络攻击事件示范演练剧本

演练概要			
演练时间	YYYY-MM-DD	演练地点	××单位网站系统所在机房
演练目的	检验××单位互联网安全防护能力，验证应急预案和应急处置流程，完善与各关联单位的应急响应联动机制。		
场景设置	某工作日，××单位发现门户网站访问缓慢，经判断为遭遇 DDoS 攻击，紧急启动应急预案并协调网络运营商开展应急处置。		
演练形式	□桌面推演　□实操演练　■示范演练	■跨行业　□跨地区　□单位内部　□部门内部	□综合演练　■专项演练
管理部门	××单位	参演机构	网络运营商、CNCERT、安全厂商
参演团队构成（单位、角色、职责分工）	指挥组：技术部门分管领导、技术部负责人、综合部负责人 策划组：技术部负责编写方案、组织策划 保障组：技术部负责安全保障（明确到人） 督导组： 观察组：行业所有单位、有关外联单位 评估组：系统运行部、综合部、行业信息安全专家组成评估小组		
演练保障	技术保障：演练相关网络设备数量、型号，拟使用的监控及处置相关工具。如入侵检测系统、防火墙系统、防病毒系统等 人员保障：信息安全运维人员及演练有关技术人员全员到岗 经费保障：应急演练预算 物资保障： 场地保障：故障模拟场地、应急指挥场地、应急处置场地等 通信保障：热线、视频会议系统、电话会议系统、其他通信设施等 其他：		

表 D.10（续）

演练方案剧本									
演练阶段	序号	演练主线（按方案步骤执行）	场景展示（镜头）	角色	指令/报告/应答	动作	同步场景	角色/动作	备注
演练开始	1	××单位向演练现场下达演练开始指令	会议室（应急指挥中心）	演练总指挥	技术部请准备开始网络攻击事件应急演练		技术部收到演练开始指令	技术部负责人	
演练开始	2	网络运营商向演练单位发起故障				向演练单位发起DDoS攻击			
故障预警、响应及报告流程	3	××单位运维部门监控出现门户网站流量告警，运维人员对告警进行初步分析，判断为门户网站遭遇DDoS攻击	机房监控室	运维人员		查看告警界面			
	4	监控人员向运维负责人报告故障	机房监控室	运维人员	报告：当前监控系统出现流量告警，经初步分析，判断为我单位门户网站遭遇DDoS攻击，建议按要求立即启动应急预案	向负责人电话报告	同意启动应急预案	技术部负责人	
应急决策、指挥、处置、报告、信息发布	5	运维负责人召集应急工作小组，进一步确认故障及影响范围，研判风险，并确定启动相应应急预案	会议室（应急指挥中心）	技术、综合、业务等部门负责人	我单位门户网站遭遇DDoS攻击，技术部门已按要求启动应急预案，通知运营商开展流量清洗工作，请各部门研判风险提出有关建议				
	6	按应急预案，紧急与运营商沟通启动流量清洗服务	机房监控室	运维人员	我单位门户网站遭遇DDoS攻击，请立即启动流量清洗服务	与运营商电话沟通	立即启动流量清洗服务	运营商	

表 D.10（续）

演练阶段	序号	演练主线（按方案步骤执行）	场景展示（镜头）	角色	指令/报告/应答	动作	同步场景	角色/动作	备注
应急决策、指挥、处置、报告、信息发布	7				我单位门户网站遭遇DDoS攻击，请立即赶赴现场配合开展应急处置	与安全服务厂商电话沟通	立即派技术人员赶赴现场	安全服务厂商	
	8	运营商流量清洗完成，网络流量恢复正常，门户网站恢复访问	运营商运管中心	运营商操作人员	已完成流量清洗工作，请确认网站是否访问正常	与××单位电话沟通	通过监控确认流量正常，网站恢复正常访问，持续跟踪	××单位运维人员	
	9	持续跟踪门户网站运行情况，并向运维负责人报告情况	机房监控室	运维人员	运营商已完成流量清洗，目前监控显示流量正常，网站恢复正常访问，请指示	向负责人电话报告	要求进一步跟踪网站运行情况	技术部负责人	
	10	与CNCERT沟通请求提供网络攻击溯源服务	机房监控室	运维人员、安全服务厂商	××单位门户网站于今日×点×分遭遇DDoS攻击，经过运营商流量清洗工作目前流量已恢复正常，网站恢复正常访问，请配合开展溯源工作	与CNCERT电话沟通	开展攻击溯源（结果后续反馈）	CNCERT	
应急演练完毕及报告、点评	11	对事件发生和应急处置概况等进行总结	会议室（应急指挥中心）	演练总指挥					
	12	专家点评，宣布演练结束	会议室（应急指挥中心）	专家					

表 D.11　网络攻击事件示范演练记录单

<table>
<tr><td colspan="8">演练概要</td></tr>
<tr><td>演练时间</td><td colspan="2">YYYY-MM-DD</td><td>演练地点</td><td colspan="4">××单位网站系统所在机房</td></tr>
<tr><td>演练目的</td><td colspan="7">检验××单位互联网安全防护能力，验证应急预案和应急处置流程，完善与各关联单位的应急响应联动机制</td></tr>
<tr><td>场景设置</td><td colspan="7">某工作日，××单位发现门户网站访问缓慢，经判断为遭遇 DDoS 攻击，紧急启动应急预案并协调网络运营商开展应急处置</td></tr>
<tr><td>演练形式</td><td colspan="2">□桌面推演　□实操演练　■示范演练</td><td colspan="3">■跨行业　□跨地区　□单位内部　□部门内部</td><td colspan="2">□综合演练　■专项演练</td></tr>
<tr><td>管理部门</td><td colspan="2">××单位</td><td>参演机构</td><td colspan="4">网络运营商、CNCERT、安全厂商</td></tr>
<tr><td colspan="8">演练记录</td></tr>
<tr><td>演练阶段</td><td>序号</td><td>起止时间</td><td colspan="2">演练过程控制情况</td><td>参演人员表现</td><td>意外情况及其处置（选填）</td><td>记录人</td><td>记录手段</td></tr>
<tr><td>系统准备及启动</td><td>1</td><td>YYYY-MM-DD
9：00-9：02</td><td colspan="2">■系统备份等安全控制措施
■演练前是否向指挥组确认
■指挥组是否正式宣布演练开始
□其他（请补充说明）</td><td>良好</td><td>无</td><td>×××</td><td>■文字
■照片
■音像
□其他（补充说明具体手段）</td></tr>
<tr><td>演练执行</td><td>2</td><td>YYYY-MM-DD
9：03-9：30</td><td colspan="2">■演练指挥组组长是否对演练全过程进行控制或授权策划组控制
■各参演机构是否按照演练预案进行事件场景模拟
■演练单位是否指定专人按预案要求将发现的问题和处置情况向总指挥部报告
■各参演机构是否将演练进展情况及时向总指挥报告
■演练执行过程是否做好全演练执行过程记录
□其他（请补充说明）</td><td>良好</td><td>无</td><td>×××</td><td>■文字
■照片
■音像
□其他（补充说明具体手段）</td></tr>
<tr><td>演练结束与终止</td><td>3</td><td>YYYY-MM-DD
9：31-9：35</td><td colspan="2">■演练结束后，是否由总指挥部宣布演练结束，且所有人员停止了演练活动
■各参演机构和指挥机构是否及时总结
■各参演机构和指挥机构对演练现场是否进行清理
□演练过程中出现突发相关情形，指挥组是否提前终止演练
□其他（请补充说明）</td><td>良好</td><td>无</td><td>×××</td><td>■文字
■照片
■音像
□其他（补充说明具体手段）</td></tr>
</table>

表 D.11（续）

演练阶段	序号	起止时间	演练过程控制情况	参演人员表现	意外情况及其处置(选填)	记录人	记录手段
系统恢复	4	YYYY-MM-DD 9:35 之后	■各参演机构是否恢复系统 ■各参演机构是否向指挥组报告系统恢复情况 ■演练结束后次日是否向指挥组书面报告系统运行状态 □其他(请补充说明)	良好	无	×××	■文字 ■照片 ■音像 □其他(补充说明具体手段)

表 D.12　网络攻击事件示范演练评估

演练概要			
演练时间	YYYY-MM-DD	演练地点	××单位网站系统所在机房
演练目的	检验××单位互联网安全防护能力，验证应急预案和应急处置流程，完善与各关联单位的应急响应联动机制		
场景设置	某工作日，××单位发现门户网站访问缓慢，经判断为遭遇 DDoS 攻击，紧急启动应急预案并协调网络运营商开展应急处置		
演练形式	□桌面推演　□实操演练　■示范演练	■跨行业　□跨地区　□单位内部　□部门内部	□综合演练　■专项演练
管理部门	××单位	参演机构	网络运营商、CNCERT、安全厂商

评估组成员			
姓名	单位	职务	专长领域
×××	××单位技术部	部门负责人	……
×××	××单位综合部	部门负责人	……
×××	网络运营商	部门负责人	……
×××	CNCERT	部门负责人	……
×××	安全服务厂商	部门负责人	……
……	……	……	……

表 D.12（续）

演练评估				
序号	评估项目	评估指标	评估结论 （1—差、3—合格、5—优秀）	改进建议
1	演练方案可行性	◆演练方案的合理性，可用性 ◆演练方案与预案符合程度	演练方案合理，与预案基本符合，得分：3	建议根据演练情况进一步修订完善预案
2	监控告警能力	◆告警信息是否及时、准确	及时、准确，得分：5	
3	故障定位能力	◆是否准确定位故障点 ◆是否及时根据预案提出解决方案	能够根据告警信息及时定位故障点并按照预案确定处置方案，得分：3	建议持续丰富和细化预案场景库
4	现场指挥协调能力	◆现场是否迅速建立应急指挥部 ◆是否有明确的指挥组和协调组 ◆指挥组和协调组命令下达是否正确 ◆各主管部门是否迅速到位，每个人员标志清楚	组织架构明确，各方响应迅速，得分：5	
5	参演人员处置能力	◆是否就位迅速，职责明确 ◆是否处置及时 ◆是否正确向指挥部反馈处置情况	应急过程中各方职责分工清晰，处置迅速且及时向指挥部反馈处置进展，得分：5	
6	关联方应急联动能力	◆接口部门及人员是否明确 ◆是否响应及时 ◆配合是否流畅	与关联方对接顺利，各关联方配合及时准确，得分：3	持续完善关联单位之间联络机制
7	演练保障能力	◆应急人员（主备岗）是否及时就位 ◆技术备品备件是否充足 ◆应急物资及必要通信设备准备是否充足 ◆是否制定意外情况应急措施和回退方案	制定了紧急情况回退方案，应急人员、设备、物资等充足，得分：5	
8	演练目标的实现情况	◆是否通过演练发现待改进事项 ◆是否达到预期目标	已针对需要改进事项提出有关建议，经评估，演练达到预期目标，得分：5	
9	演练的成本效益分析	◆是否符合演练预算，厉行节约	严格按照预算开展演练，得分：5	

表 D.13　网络攻击事件示范演练总结

演练概要			
演练时间	YYYY-MM-DD	演练地点	××单位网站系统所在机房
演练目的	检验××单位互联网安全防护能力，验证应急预案和应急处置流程，完善与各关联单位的应急响应联动机制		
场景设置	某工作日，××单位发现门户网站访问缓慢，经判断为遭遇 DDoS 攻击，紧急启动应急预案并协调网络运营商开展应急处置		
演练形式	□桌面推演　□实操演练　■示范演练	■跨行业　□跨地区　□单位内部　□部门内部	□综合演练　■专项演练
管理部门	××单位	参演机构	网络运营商、CNCERT、安全厂商
演练评估			
演练评估时间	YYYY-MM-DD	演练评估地点	××单位会议室
评估专家组成员	××单位技术部、综合部及有关业务部门负责人、网络运营商、CNCERT、安全厂商有关负责人		
评估结论	演练方案涉及合理，与预案基本符合； 告警及时、准确，能够根据告警信息及时定位故障点并按照预案确定处置方案； 组织架构明确，各方响应迅速，职责分工清晰，处置迅速； 与关联方对接顺利，各关联方配合及时有效； 达到预期演练目标		
演练总结及改进思路			
演练总结	将于演练结束两周内编制详细演练总结及整改方案		
改进思路	将于演练结束两周内编制详细演练总结及整改方案		

参 考 文 献

[1] GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南
[2] GB/T 24363—2009 信息安全技术 信息安全应急响应计划规范
[3] 国家网络安全事件应急预案(中网办发文〔2017〕4号)