

ICS 35.100.70

L 79

YD

中华人民共和国通信行业标准

YD/T 2880-2015

域名服务业务连续性管理要求

Requirements for domain name service
business continuity management

2015-07-14 发布

2015-10-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
引 言	III
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
4 概述	4
5 业务连续性管理方针	5
6 业务影响分析	5
7 风险评估	9
8 业务连续性管理策略	9
9 业务连续性管理响应	11
10 业务连续性方案管理	14
11 顶级域名注册管理机构要求	15
参考文献	17

前 言

本标准是“域名系统运行技术规范体系”系列标准之一，该系列标准的结构及名称如下：

- YD/T 2135 《域名系统运行总体技术要求》；
- YD/T 2138 《域名系统权威服务器运行技术要求》；
- YD/T 2137 《域名系统递归服务器运行技术要求》；
- YD/T 2140 《域名服务系统安全框架技术要求》；
- YD/T 2139 《IPv6 网络域名服务器技术要求》；
- YD/T 2136 《域名系统授权体系技术要求》；
- YD/T 2052 《域名系统安全防护技术要求》；
- YD/T 2053 《域名系统安全防护检测要求》；
- YD/T 2091 《公共域名解析系统安全要求》；
- YD/T 2880 《域名服务业务连续性管理要求》。

本标准按照 GB/T 1.1-2009 给出的规则起草。

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。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国互联网络信息中心、工业和信息化部电信研究院、政务和公益机构域名注册管理中心。

本标准主要起草人：徐 颖、王 伟、胡安磊、李晓东、刘 越、王 正。

引 言

随着互联网的不断发展,域名服务作为互联网重要的基础设施也成为影响互联网安全稳定的重要因素。对域名服务来说,保障其“可用性”是其核心目标,对域名服务实现业务连续性管理是保障可用性的最佳方式。互联网名称与数字地址分配机构(ICANN)在新通用顶级域名(New gTLD, New Generic Top-level Domain)的申请指南中就明确提出要求顶级域名注册管理机构制订业务连续性计划并配备相关的实施条件。

由于国际上通用的业务连续性管理标准并不能完全符合我国域名服务的实际情况,因此,在参考国际通用标准的基础上,依据我国域名服务实践,建立清晰明确的要求,从操作层面上提供互联网域名服务业务连续性管理的客观标准和执行方法,指导域名服务组织进行业务连续性管理,对整个域名行业的发展具有十分重要的意义。

本标准各类域名服务组织提供了实施业务连续性管理的方法,对顶级域名注册管理机构提出具体的业务连续性管理指标要求,以进一步提高域名服务组织的持续服务能力,提高各项域名服务的可用性水平,从而为我国互联网基础设施的安全稳定运行提供更好的保障。

域名服务业务连续性管理要求

1 范围

本标准规定了域名服务组织针对其域名业务进行业务连续性管理时的技术要求，适用于国内相关企业事业单位开展的互联网域名服务业务。这些域名服务组织覆盖域名服务体系的各个环节，包括根域名服务器管理机构、顶级域名注册管理机构、域名注册服务机构、其他重要权威域名服务组织、重要递归域名解析服务机构。

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，仅所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。

YD/T 1730 电信网和互联网安全风险评估实施指南

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

权威域名解析系统 Authoritative Domain Name Service System

对于某个或者多个区具有权威的服务系统，权威解析服务系统保存着其所拥有权威的区的原始域名资源记录信息。根据域名系统名字空间的树状结构，权威域名解析系统包括根域名解析系统、顶级域名解析系统和其他各级域名解析系统。

3.1.2

递归域名解析系统 Recursive Domain Name Service System

负责接收用户（解析器）的解析请求，并通过查询本地缓存或者执行从根域名解析系统到被查询域名所属权威服务系统的递归查询过程，获得解析结果并返回给用户的域名解析系统。一般来说，按照职能的不同，域名解析服务系统本身可以分为权威解析服务系统和本地递归解析服务系统两类。这两者之间最大的区别就是，权威解析服务系统通常不提供递归解析（Recursive Resolution）服务，它只负责维护和保存它所拥有权威的区的资源记录信息，并且接受递归解析服务系统的查询请求；而本地（递归）解析服务系统则通常不会维护或者管理任何区的资源记录数据，它只负责接收用户的查询，并且通过本地缓存或者向包括根在内的权威名字服务系统发出查询从而获得查询结果。

3.1.3

区文件 Zone File

某个区内的域名和资源记录及相关的权威起始信息（Start of Authority, SOA）按照一定的格式进行组合，从而构成存储这些信息的区文件。其中，权威起始信息包含了区的管理员电子邮件地址（Mail Address）、序列号（Serial）、更新周期（Refresh）、重试周期（Retry）和过期时间（Expire）等信息。

3.1.4

数据托管 Data Escrow

域名服务组织向作为中立第三方的数据托管机构定期备份数据，以保证在域名服务组织停止运营、灾难等情况下不能对外提供域名服务时，可以由业务接管机构使用备份数据进行业务接管。数据托管机构应由政府主管部门或ICANN认证，具备相应资质，例如ICANN认证的、针对新通用顶级域名注册管理机构和注册服务机构的数据托管代理（Data Escrow Agent）等。

3.1.5

业务接管 Service Take-Over

在域名服务组织停止运营、灾难等情况下不能对外提供域名服务时，由业务接管机构使用备份数据重建域名服务系统，接管域名服务业务。域名服务组织应选择由政府主管部门或ICANN认证的、具备资质的业务接管机构，例如ICANN认证的、针对新通用顶级域名注册管理机构和注册服务机构的紧急后台注册管理执行机构（Emergency Back-end Registry Operator EBERO）等。

3.1.6

组织 Organization

由不同作用的个体为实施共同的业务目标而建立的结构，组织的特性在于为完成目标而分工、合作；一个单位是一个组织，某个业务部门也可以是一个组织。

3.1.7

事故 Incident

可能引起业务中断或其他损失的情形。

3.1.8

灾难 Disaster

由于人为或自然的原因，造成信息系统严重故障或瘫痪，使信息系统支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

3.1.9

业务连续性 Business Continuity

组织对事故和业务中断的规划和响应，使业务能在预设的水平上持续运行的策略和能力。

3.1.10

业务连续性管理 Business Continuity Management (BCM)

为保护组织的利益、声誉、品牌和价值创造活动，找出对组织有潜在影响的威胁，提供建设组织有效反应恢复能力的框架的整体管理过程。包括组织在面临灾难时对恢复或连续性的管理，以及为保证业务连续性计划有效性的培训、演练和检查的全部过程。

3.1.11

业务连续性计划 Business Continuity Plan (BCP)

组织所开发和维护的一套程序计划，以使组织在事故发生时能够在一个预定的可接受的水平上继续提供其关键活动。

3.1.12

业务连续性策略 Business Continuity Strategy

组织在发生事故或业务中断时保证业务连续的方法。

3.1.13

业务影响分析 Business Impact Analysis (BIA)

分析业务功能及相关信息系统资源、评估特定灾难对各种业务功能的影响的过程。

3.1.14

恢复时间目标 Recovery Time Objective (RTO)

灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求。

注：可简单的理解为灾难发生后，组织能够容忍多长时间的业务中断时间。

3.1.15

恢复点目标 Recovery Point Objective (RPO)

灾难发生后，系统和数据必须恢复到的时间点要求。

注：可简单的理解为灾难发生后，组织能够容忍丢失多长时间的数据量。

3.1.16

关键业务 Critical Business

如果中断一定时间，将显著影响组织运作的服务或职能。

3.1.17

关键活动 Critical Activities

组织产品或服务所必需执行的活动。

3.1.18

演练 Exercise

对业务连续性计划的部分或全部内容进行预演，以保证计划真正付诸实施时能够达到预期效果。

注：演练可能会真正启动业务连续性计划，但更多可能是模拟一个事故，通过评估参与者角色的操作，来发现可能出现的问题并进行改正。

3.1.19

事故管理计划 Incident Management Plan (IMP)

明确定义的用来用来应对和处置事故的计划文件，通常包括实施事故管理过程所需的关键人员、资源、服务或活动。

3.1.20

启动 Invocation

组织宣布业务连续性计划需要付诸实施，以继续提供关键产品和服务。

3.1.21

重续 Resumption

灾难备份中心替代主数据中心，支持关键业务重新运作的过程。

3.1.22

健壮度 Resilience

组织承受事故影响的能力。

3.1.23

风险评估 Risk Assessment

风险识别、风险分析和风险评价的整个过程。

3.1.24

利益相关方 Stakeholders

组织成果的所有既得利益获得方。

3.1.25

最高管理层 Top Management

在组织的最高层实施指导和控制的个人或小组。

注：在大型组织，最高管理者可不直接参与，但其他管理者需要通过行政管理系统承担相应职责；在小型组织，业主或经营者可作为最高管理层。

3.2 缩略语

下列缩略语适用于本文件。

DDOS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name System	域名系统
DOS	Denial of service	拒绝服务
BCM	Business Continuity Management	业务连续性管理
BCP	Business Continuity Plan	业务连续性计划
BIA	Business Impact Analysis	业务影响分析
IMP	Incident Management Plan	事故管理计划
RTO	Recovery Time Objective	恢复时间目标
RPO	Recovery Point Objective	恢复点目标
ICANN	The Internet Corporation for Assigned Names and Numbers	互联网名称与数字地址分配机构

4 概述

业务连续性管理是一个由业务而非技术驱动的过程，目标是建立符合预定业务连续性目标的战略和操作框架，其目的一般包括：

- 提高组织抵抗业务中断的能力。
- 为事故发生后组织在预设时间内按预设水平恢复提供其关键产品或服务的能力提供方法。
- 展示经过证明的管理业务中断的能力，以保护组织的信誉和品牌。

而随着互联网的不断发展，域名服务作为互联网重要的基础设施也成为影响互联网安全稳定的重要因素。对域名服务来说，保障其“可用性”是其核心目标，对域名服务实现业务连续性管理是保障域名服务可用性、抵抗并管理业务中断的最佳方式。域名服务组织应参照本标准实施业务连续性管理，满足标准相关要求。

参考业务连续性管理国际标准和中國域名服务运营经验，结合域名服务的现实情况和发展趋势，域名服务组织实施业务连续性管理主要包括如下内容：

- 业务连续性管理方针：建设组织在业务连续性管理上的整体方针文件。
- 业务影响分析：通过业务影响分析识别组织的关键业务和关键活动，分析其中断影响，从而制订业务连续性管理目标。

c) 风险评估：识别业务所面临的主要风险并进行处置。

d) 业务连续性管理策略：为保证业务连续性管理目标的实现，采取必要的管理和技术策略，以减少业务中断的可能、降低业务中断的损失、加快业务中断后的恢复等。

e) 业务连续性管理响应：建设相应的预案和流程，规范组织在面临业务中断时的响应措施。

f) 业务连续性方案管理：为保证业务连续性所进行的培训、演练、评审、记录和文件管理等工作。

5 业务连续性管理方针

为保证域名服务的业务连续性管理工作顺利开展，域名服务组织应该建设业务连续性管理方针（BCM 方针）文件，目的是：

a) 保证所有业务连续性管理工作的正常实施和运行；

b) 让业务连续性能力满足不断变化的业务要求，并与组织的规模、复杂程度和性质相匹配；

c) 为持续的业务连续性管理建设清晰的框架。

BCM 方针作为一个纲领性文件，应为域名服务组织的业务连续性管理指明纲领性的原则，阐述组织对域名服务的业务连续性管理目标，明确业务连续性管理所覆盖的范围，并致力于业务连续性能力的测量。BCM 方针应由组织的最高管理层批准，并定期或在发生重大变化时及时进行评审、修订和发布。

组织在开发 BCM 方针时，可考虑以下因素：

a) 确定组织内的业务连续性管理实施范围；

b) 业务连续性管理所需资源的获得及管理者承诺；

c) 为组织定义业务连续性管理的原则、指南以及最低标准；

d) 相关参考标准、法规或政策；

e) 根据组织需要，定期评审和维护 BCM 方针及其他业务连续性管理计划和方案；

f) BCM 方针应清晰说明例外和使用限制。

6 业务影响分析

6.1 业务影响分析的内容

域名服务组织应该通过文件化的业务影响分析识别业务连续性管理的具体对象——关键业务和关键活动，并制订业务连续性管理的关键目标——RTO 和 RPO 指标。

6.2 关键业务识别

域名服务组织应识别所运营的各项关键域名业务。这些关键业务包括域名解析、域名注册、域名查询、数据托管等，以及其他与域名直接或间接相关的业务，例如客户服务等。针对一个域名业务，还应继续识别业务运营所需要的至关重要的、必须履行的活动，称之为关键活动。

在进行组织关键业务及关键活动的识别时，域名服务组织可以根据组织实际情况，对组织所有业务及活动根据其重要程度进行分级，从而识别哪些业务/活动对组织是关键，需要进行业务连续性管理，哪些业务/活动相对不关键，可以不进行业务连续性管理，或按重要级别分步骤逐步实施业务连续性管理。同时，业务/活动的分级也可以作为事故发生后各业务/活动的恢复优先级，从而在事故情况下最优先恢复最重要的业务/活动。

业务/活动分级方法示例见表1。

表 1 业务及活动分级方法

级别	分级标准
一级	<ul style="list-style-type: none"> 直接面对客户或合作伙伴提供服务 关系到国家互联网安全 关系到组织生存 属于组织核心职责
二级	<ul style="list-style-type: none"> 直接面对客户或合作伙伴提供服务 对组织收入、业务开展、品牌形象有较严重的影响 属于组织核心职责
三级	<ul style="list-style-type: none"> 对组织收入、业务开展、品牌形象有一定的影响 属于组织的扩展业务，或用来支撑组织核心职责的业务
四级	<ul style="list-style-type: none"> 重要内部应用业务或部门级对外服务业务
五级	<ul style="list-style-type: none"> 其他业务，没有业务连续性要求，不需要进行业务连续性管理

对不同类型的域名服务组织，可能识别出的关键域名业务及关键活动见表2（一个组织可以承担多个类型组织的职责）。

表 2 关键业务及关键活动

域名服务组织	关键业务	关键活动
顶级域名注册管理机构	顶级域名解析	Zonefile 文件生成和分发； DNS 解析
	域名注册	接收域名注册申请； 域名注册审核
	域名查询	WhoisD； Whois Web； Whois 批量访问 ^a ； 可搜索的 Whois ^b
	数据托管	托管数据生成； 托管数据传送给数据托管机构
	财务	注册服务机构续费
域名注册服务机构	域名注册	接收用户域名注册申请； 域名注册申请提交给顶级域名注册管理机构
	权威域名解析	Zonefile 文件生成和分发； DNS 解析
	数据托管	托管数据生成； 托管数据传送给数据托管机构
其他重要权威域名服务组织	权威域名解析	Zonefile 文件生成和分发； DNS 解析
	数据托管	托管数据生成； 托管数据传送给数据托管机构
重要递归域名服务组织	递归域名解析	DNS 解析

注^a 顶级域名注册管理机构对授权第三方提供 Whois 批量访问查询功能，允许其在特定时间段内批量访问 Whois 数据。

注^b 顶级域名注册管理机构对授权互联网用户提供查询功能，可以按照域名、注册人姓名、邮编地址、联系人姓名、注册服务商 ID 和互联网协议地址作为关键词，并通过 AND/OR/NOT 的 Boolean 功能，实现基于任意关键词组合的搜索

不同类型域名服务组织及其关键业务之间的关系如图1所示。

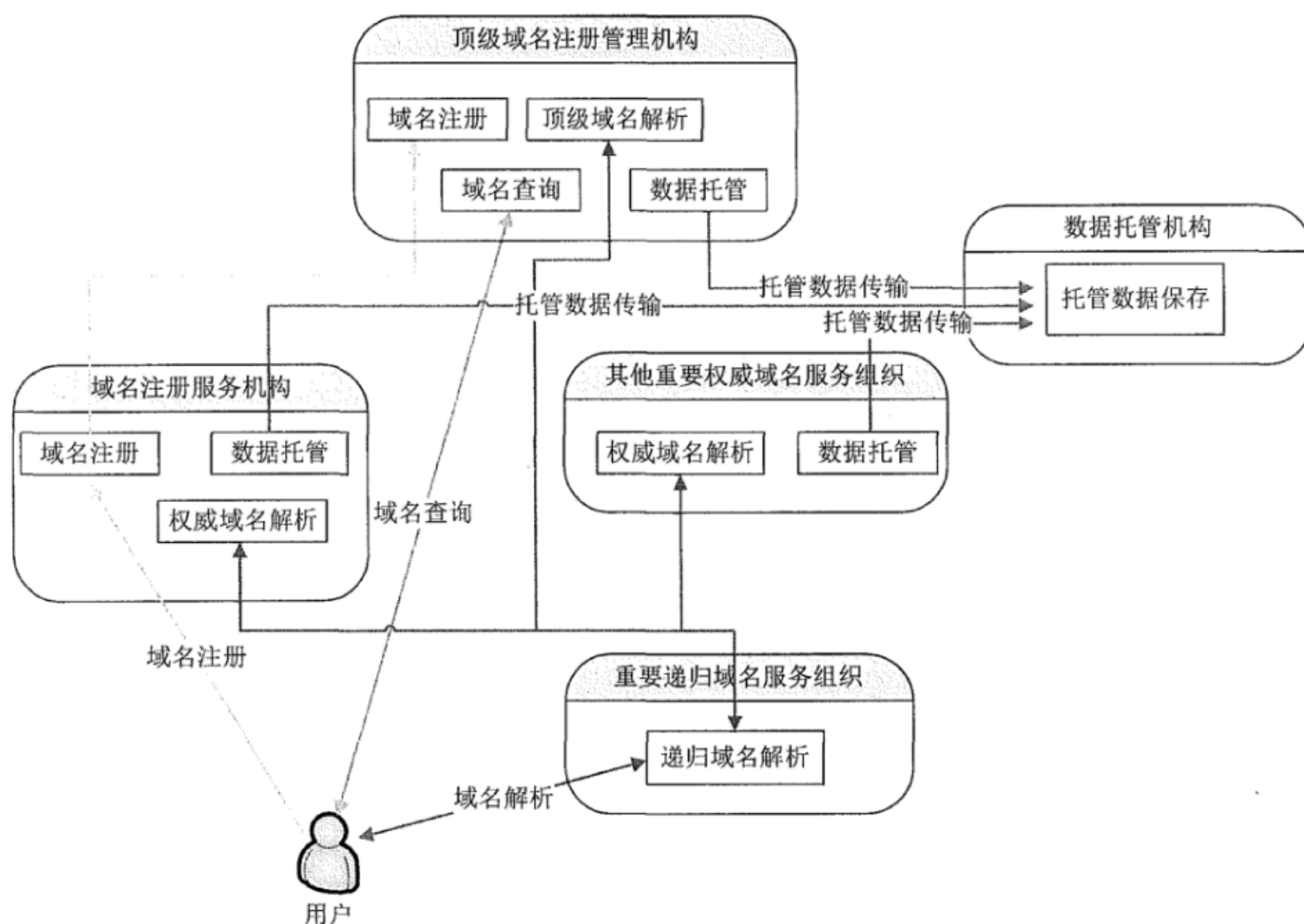


图1 域名服务组织关系示意

对关键业务和关键活动，域名服务组织应该识别所需要的资源，通过业务连续性管理保证资源的可用。这些资源可能包括以下内容。

- a) 人员：域名业务/活动开展所必需的员工资源，包括人、技能和知识。
- b) 基础设施：必要的办公场所和办公设施。
- c) 技术设施：用于支持业务活动的域名服务系统，包括域名服务系统所依赖的物理场所、网络环境、软硬件等。
- d) 信息：域名业务/活动所依赖的数据。
- e) 外部资源：外部提供的服务和资源供应。

6.3 业务中断影响分析

业务中断影响分析，主要考虑业务中断后在不同层面的影响，以及随中断时间的推移影响程度的变化。业务中断影响分析的评估方法、发现和结论应形成文档。业务中断时间可以是一段时间内业务始终不能提供，或期间业务断续中断或服务质量很差导致组织认为此段时间内业务无法正常开展。

业务中断影响分析可以使用如下的定性非财务影响分析或定量财务影响分析，域名服务组织可以根据组织情况自行选择一种方法或同时使用两种方法综合进行分析。

- a) 非财务影响分析通过定性评估的方式，在不同层面给业务中断不同时间后的影响赋值（例如5分制，0分无影响，3分中等影响，5分影响最大），在确定何种级别的影响是不可以接受之后，逐一从不同

层面形成RTO需求，后续再综合考虑各层面的RTO需求综合形成业务/活动的RTO指标。例如可以考虑如下一个或几个层面的影响：

- 国家网络安全；
- 社会影响程度；
- 客户满意度；
- 组织品牌声誉；
- 组织业务运营；
- 其他。

对一项业务/活动中断的非财务影响分析方法示例见表3。

表3 业务中断非财务影响分析

对象	中断时间					
	1h	4h	8h	24h	72h	RTO 需求
国家网络安全						
社会影响程度						
客户满意度						
组织品牌声誉						
组织业务运营						

b) 财务影响分析需要识别财务损失金额随中断时间变化，财务损失包括收入损失、罚金和赔偿金等，形成业务收益损失的量化评估模型。对一项业务/活动中断的财务影响分析示例如图2所示。

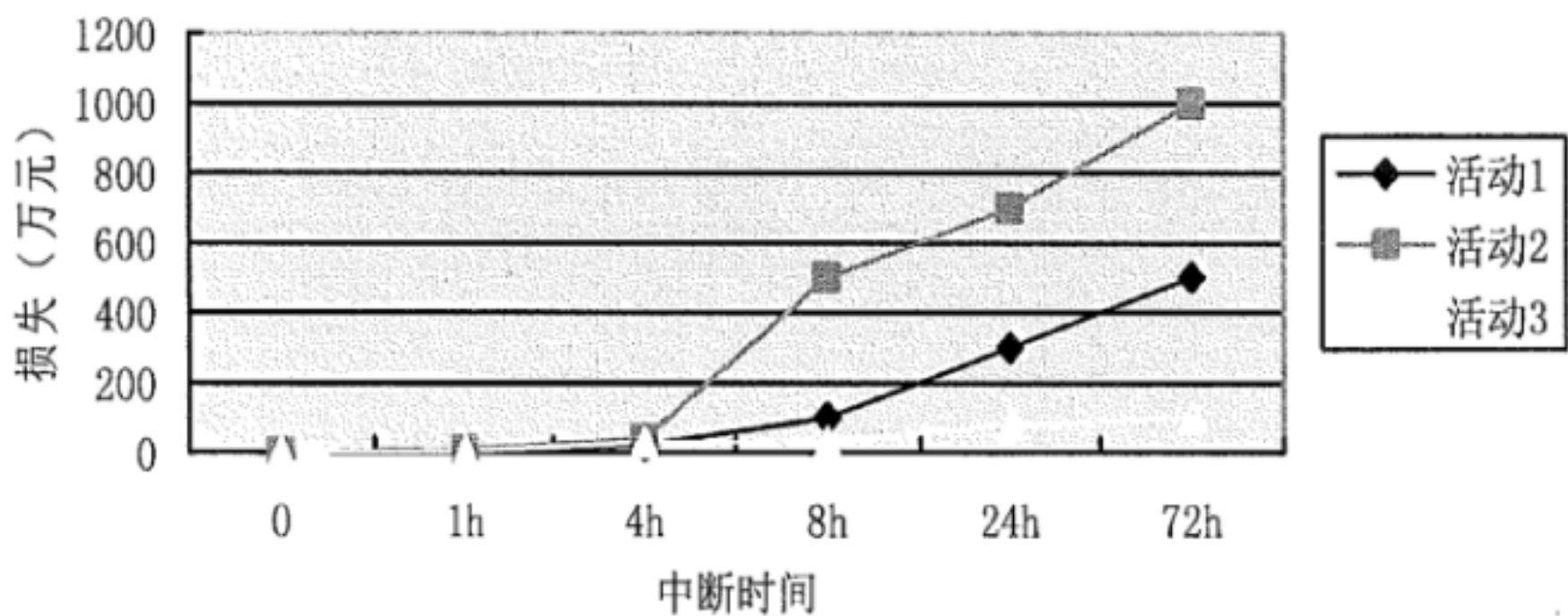


图2 业务中断财务影响分析

6.4 RTO 和 RPO 指标

根据上节业务中断影响分析中非财务影响和财务影响的综合判断，域名服务组织通过讨论确定不可接受的业务中断时间和数据丢失时间，即RTO指标和RPO指标。RTO和RPO指标的制订除了考虑业务中断的影响外，还需考虑达到目标所需要投入的成本，通过成本效益分析确定适合于域名服务组织的合适目标。

RTO指标和RPO指标及可以针对每一个业务制定，也可以针对业务的每一个关键活动制定。

组织应通过后续业务连续性管理策略和业务连续性管理响应的实施，在业务中断情况下在RTO指标时间内恢复业务/活动运行，并明确每一业务/活动恢复运转的最低级别，以及保证最多只能丢失RPO指标时间段的数据。

RTO和RPO指标应由最高管理层批准，并作为组织目标并给予资源支持。

7 风险评估

风险评估工作是业务连续性管理工作的一部分，域名服务组织应针对所识别的关键业务、关键活动及所依赖的资源进行风险评估和风险处置。

风险评估应包括如下要素：

- a) 制定接受风险的准则；
- b) 识别可接受的风险级别；
- c) 识别所面临的威胁；
- d) 识别可能被威胁利用的脆弱点；
- e) 识别风险可能造成的影响。

风险评估的方法见YD/T 1730。

域名服务组织进行风险评估所识别出的不可接受风险，是建设业务连续性管理策略（如第8章所述）时所考虑的重要因素，业务连续性管理策略应致力于降低这些风险，寻求提高业务/活动的健壮度，保证关键业务/活动按所规定的最低可接受水平持续运行，以及在业务中断情况下及时重续、恢复业务。

8 业务连续性管理策略

8.1 概述

域名服务组织应建设业务连续性管理策略（BCM策略），落实关键业务/活动所需要的资源，以支持关键业务/活动的RTO、RPO指标实现。

确定BCM策略应该考虑达成如下目标：

- a) 实施合适的措施以降低事故发生的可能性或降低这些事故的影响，增强关键业务/活动的健壮度；
- b) 在事故中和事故后保障关键业务/活动的连续性。

组织应为关键业务/活动制定合适的BCM策略，并配备关键业务/活动恢复所需的资源。选择最为合适的策略时需考虑如下要素：

- a) 关键业务/活动中断的最大可容忍期限；
- b) 策略实施的成本；
- c) 不采取行动的后果。

8.2 人员

域名服务组织应建立管理核心技能、知识以及相应人员的合适策略，以保证在灾难情况下重要人员和核心技能的持续可用，这些人员包括内部员工、外包人员以及其他拥有广泛特殊技能和知识的利益相关方。所需要采取的策略可能包括：

- a) 对关键域名业务和活动的运行维护形成文件，减少对具体人员的直接依赖；
- b) 对员工和外包人员进行充分的多种技能培训，使人员掌握多种技能，互相备份；
- c) 分离关键技能和职责，以防止风险集中，例如对拥有核心技能的员工实现物理分离（不同办公区域、甚至不同城市），或保证超过一人拥有核心技能可以履行核心职责；
- d) 利用第三方资源提供人员和技能备份；
- e) 建立人才储备计划，以便必要时应急招聘人员；

f) 通过知识管理保证域名业务和活动相关知识在组织内的传承。

8.3 基础设施

域名服务组织基础设施主要指必要的办公场所和办公设施，组织应该建立相应策略以降低其正常工作环境不可用所造成的影响。所需要采取的策略可能包括如下一项或多项：

- a) 组织建设自有的备用工作场所（包括办公设施），支持工作人员转移至此开展域名业务、活动；
- b) 由合同/协议约定的其他组织或第三方专门机构提供备用基础设施，支持工作人员转移至此开展域名业务、活动；
- c) 组织提供支持家庭或远程办公的技术手段，工作人员可以在家庭或其他地点开展域名业务、活动；
- d) 必要时在已确定的备用场所中配备备用人力，可以迅速重续服务。

8.4 技术设施

域名服务技术设施主要包括用于支持业务活动的域名服务系统，以及域名服务系统所依赖的物理场所、网络环境、软硬件等。域名服务系统通常需要复杂的连续性策略来保证系统的可用性，以支持域名业务/活动的恢复时间目标（RTO）。根据RTO指标的不同，所需要采取的策略也会有所不同，这些策略可能包括：

- a) 为域名服务系统提供同城或异地的灾备系统，以在必要情况下使用灾备系统重续服务。灾备系统设置应考虑如下问题：
 - 灾备系统的处理能力需要达到何种程度；
 - 两个地点的物理距离可能会给域名服务系统的运行和切换带来的负面影响；
 - 备用域名服务系统启用需要人工干预还是自动启用。
- b) 对域名服务系统进行分布式部署，提供充分的地理冗余度。
- c) 域名服务系统设备的处理能力应具备一定的冗余，对关键设备的重要部件、关键设备、重要线路、网络接入均采用冗余的方式提供保护，提供灾难备份和恢复的能力。
- d) 实现域名服务系统重要设备的冷备，例如保留旧设备用于紧急替换或作为备件，或要求设备供应商提供应急设备的服务等。
- e) 为域名服务系统建设流量负荷分担设计。
- f) 为域名服务系统提供远程管理功能。

8.5 信息

灾难情况下进行业务恢复时，需要将域名服务组织的信息恢复到某一状态点，因此，域名服务组织应采取信息备份策略，以支持实现恢复点目标（RPO）。这些信息主要指域名业务/活动所产生的各种数据，包括解析Zonefile文件、域名注册信息、域名服务系统日志等。

信息备份策略可采用多种不同的备份方法，例如磁带等电子介质备份、集中文件传输备份、存储级数据同步复制备份、存储级数据异步复制备份、数据库事务日志复制备份等，备份的信息可以在本地也可以在异地。具体备份策略的选择依赖于RPO指标和风险评估所识别的风险，可能的选择如下：

- a) RPO为0，使用存储级数据同步复制备份机制；
- b) RPO为0~60min，可以使用存储级数据异步复制备份、数据库事务日志备份、文件实时更新（例如inotify+rsync技术）等机制或RPO更低时的备份机制；

- c) RPO为1~24h, 可以使用文件定时传输备份等机制或RPO更低时的备份机制;
 - d) RPO大于24h, 可以使用磁带等电子介质备份等机制或RPO更低时的备份机制。
- 信息策略应该对使用备份到安全地点的信息进行恢复的方法形成文件。

8.6 数据托管

域名服务组织的BCM策略中, 除自行采取各种措施外, 还应利用数据托管服务, 向数据托管机构定期备份数据, 以保证如果灾难情况下不能自行重续服务, 可以由其他机构进行业务接管, 代为提供服务。域名服务组织应选择由政府主管部门或ICANN认证的、具备资质的数据托管机构, 例如ICANN认证的、针对新通用顶级域名注册管理机构和注册服务机构的数据托管代理 (Data Escrow Agent) 等。

域名服务组织应与数据托管机构通过合同约定数据托管服务细节, 落实数据托管策略, 这些策略包括但不限于:

- a) 域名服务组织定期 (例如每天) 向数据托管机构发送增量数据进行备份;
- b) 域名服务组织定期 (例如每周) 向数据托管机构发送全量数据进行备份。

9 业务连续性管理响应

9.1 概述

灾难发生后, 业务连续性管理响应 (BCM响应) 的阶段如图3所示, BCM响应管理覆盖事故响应、业务重续、业务恢复阶段的内容, 对应包括事故响应计划 (IMP)、业务连续性计划 (BCP)、业务恢复计划, 同时, 域名服务组织应建设相应的BCM响应组织架构来保证响应及时、有效进行。

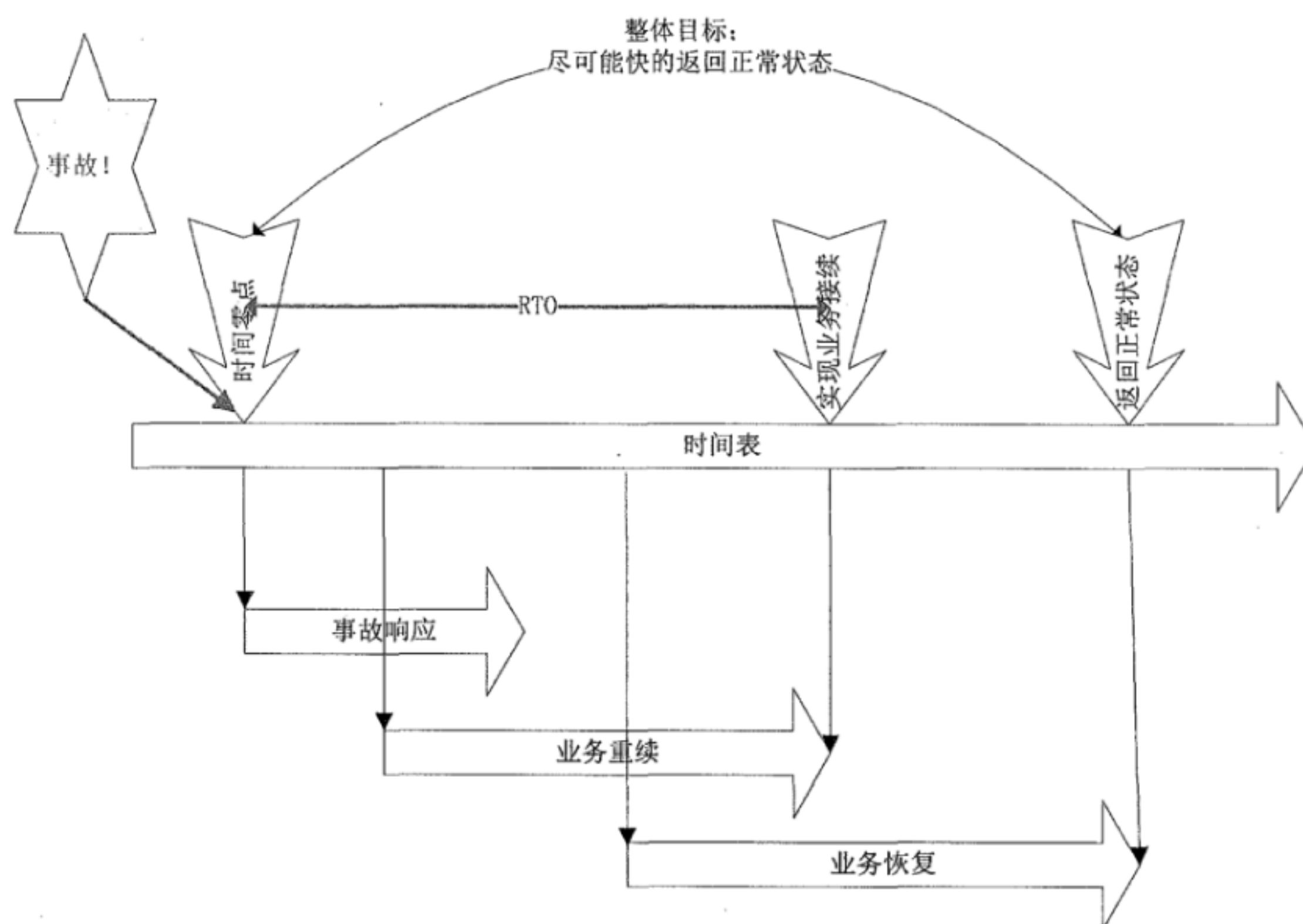


图3 业务连续性管理响应阶段

BCM响应设计一般落实为应急预案体系，域名服务组织应建设应急预案来规范BCM响应，其中，事故响应计划、业务连续性计划、业务恢复计划可以综合在一起，也可以分散为多个应急预案，但不论如何，上述计划都应该简单明了，并让在计划中定义有职责的人员可以获取。

所有计划一般都应包含以下要素。

a) 目的和范围：计划中首先定义目的和范围，获得最高管理层的认可，并获得计划实施人员的理解。目的和范围包括需要恢复的关键业务/活动、恢复时间表、关键业务/活动的恢复水平、计划适用的情形等内容。

b) 角色和责任：计划应清晰的定义事故发生时或发生后，具备相应权力的人员和小组的角色和责任。

c) 计划的启动：事故发生后，需要在尽可能短的时间启动相关计划或计划的相关部分。计划应对在什么样的条件下、谁有权启动计划、如何启动计划进行清晰的说明。

d) 文件的所有人和维护人员：组织应指定计划的主要责任人，由其负责按计划的时间间隔对计划进行评审、修订和更新。计划的修订应该引入版本控制体系，变更应通知到所有相关方。

e) 具体的联系方式：每一计划都应该包含所有关键利益相关方的具体联系方式。

9.2 组织机构

针对BCM响应管理，域名服务组织应该定义一个BCM响应组织结构，使组织能够有效响应事故并从事务中进行业务重续和恢复。

BCM响应组织结构应该能针对所有事故简单和快速进行进行响应，达成如下目标：

- a) 确认事故的性质和程度；
- b) 控制事态的进一步发展；
- c) 启动合适的业务连续性响应措施，使关键业务/活动能够重续和恢复；
- d) 与利益相关方进行及时有效沟通。

该组织结构还应该管理BCM响应相关的所有计划和预案。

域名服务组织BCM响应组织结构的成员应包括组织组织高层领导、各域名业务主管、域名服务系统相关技术主管、相关技术和业务岗位人员等。

9.3 事故响应

域名服务组织应建设事故响应计划（IMP），以对域名业务所面临的事故进行定义和分类分级，并分别针对不同的事故设计事故应急处理程序，包括必要时启动业务连续性计划。事故响应计划中应针对不同事故定义不同人员的处理操作。事故响应计划除应包括9.1节中的一般性要求外，还应包括如下内容：

a) 安全事故的定义和分类分级。

b) 不同事故处理的任务清单以及负责岗位。安全事故的处置可以根据业务和活动实际情况以及历史经验，预设不同的场景分别设计处理程序，例如外部攻击（DOS/DDOS攻击等）、机房物理环境灾难（火灾、电力中断等）、办公场所灾难、软件故障、硬件故障等。

c) 相关组织和人员的应急联系方式。

d) 媒体回应方案，包括媒体发言人、媒体窗口、事故后早期提供给媒体声明的指南和模板等。

e) 对利益相关方的管理。

9.4 业务重续

域名服务组织应利用第8章建立的BCM策略，在业务中断一定时间后启动业务连续性计划（BCP）进行业务重续，包括启用备用人员、启用备份办公场地和办公设施等基础设施、在灾难备份中心启用备份技术设施和备份数据等，从而在RTO指标内重续关键业务/活动。

业务重续可以不要求达到原来的域名业务服务水平，而只维持最低需求的服务水平，业务连续性计划中应对业务重续所应达到的服务水平目标进行明确。

除应包括9.1节中的一般性要求外，业务连续性计划还应包括相关活动列表以及活动的优先次序，具体内容应包括：

- a) 在何种情况下启动业务连续性计划，例如相应域名业务/活动已中断多长时间、或预计将中断多长时间等。启动计划的域名业务/活动中断时间应小于（RTO指标-业务重续所花费的时间），并预留一定的裕量。
- b) 谁负责决定启动业务连续性计划，以及作出决定之前应该咨询和汇报的人员；
- c) 决定启动业务连续性计划后，应该被通知的人员，以及如何通知；
- d) 启动业务连续性计划后，各个岗位进行业务重续的具体操作，包括谁需要在什么时候去哪里进行什么操作等；
- e) 业务重续过程中，可以利用哪些服务，在什么地方、什么时候可以获取此服务，包括使用外部和第三方资源等；
- f) 业务重续过程中，如何及时进行信息的沟通，包括沟通频率、沟通对象、沟通内容等。

9.5 业务接管

业务连续性计划中还应考虑到，如果在启动业务连续性计划，组织自行采取措施进行业务重续之后，灾难超出预计，域名服务组织已经不能自行在规定时间内完成业务重续，则应及时启动业务接管机构来接管业务。业务接管机构将从数据托管机构获取备份数据，利用其技术平台重建域名服务系统，接管域名服务业务。域名服务组织应选择由政府主管部门或ICANN认证的、具备资质的业务接管机构，例如ICANN认证的、针对新通用顶级域名注册管理机构和注册服务机构的紧急后台注册管理执行机构（Emergency Back-end Registry Operator, EBERO）等。

域名服务组织业务连续性计划中业务接管机构接管业务的内容应包括：

- a) 何种情况下放弃自行进行业务重续，而启用业务接管机构接管业务；
- b) 谁负责决定启动业务接管机构接管业务，以及作出业务接管决定之前应该咨询和汇报的人员；
- c) 决定启动业务接管后，应该被通知的内部人员、数据托管机构联系人员、业务接管机构联系人员，以及如何通知；
- d) 启动业务接管后，域名服务组织内部、数据托管机构、业务接管机构相关各个岗位进行业务接管的具体操作，包括谁需要在什么时候去哪里进行什么操作等；
- e) 业务接管过程中，域名服务组织、数据托管机构、业务接管机构内部及互相之间如何及时进行信息的沟通，包括沟通频率、沟通对象、沟通内容等；
- f) 完成业务接管之后，如何向主管部门、利益相关方通报业务接管情况。

9.6 业务恢复

域名服务组织在完成业务重续后，可以提供一定水平的域名业务服务。

但在事故完全处理完成，对损害进行修复或替换，域名业务现场恢复后，应将业务重新切换回正常状态，包括工作人员及工作场所的回迁、IT系统和数据切换到生产现场等。

因此，应建设业务恢复计划，使用本计划将所有业务切换到生产现场，使一切恢复正常。业务恢复计划应包括9.1中的一般要求内容，主要对业务切换过程进行规范。

10 业务连续性方案管理

10.1 培训

域名服务组织应定期开展业务连续性管理培训，提高人员的业务连续性管理意识，确保所有参与业务连续性管理的人员知道并理解其角色与责任，使相关人员具备相应的管理与技术能力。

10.2 演练

域名服务组织应通过定期演练来保证业务连续性管理满足其业务要求，特别是进行应急响应计划和业务连续性计划的演练，以保证应急响应计划和业务连续性计划的可执行性和合理性，保证计划可以正常执行并持续改进。

通过业务连续性管理演练主要可以达到如下目的：

- a) 锻炼组织的BCM响应能力；
- b) 确认现有的BCM响应计划已经覆盖了组织的所有关键业务和活动，并按正确的优先级进行排序；
- c) 找到有疑问的假定和设计；
- d) 通过对演练的宣传，提高业务连续性意识；
- e) 确认关键活动恢复的有效性和时间表；
- f) 证实业务连续性管理团队的能力。

业务连续性管理演练方式见表4。

表 4 业务连续性管理演练方式

复杂程度	演练	过程	最佳频次
简单	桌面检查	会议讨论 IMP、BCP 的内容，进行内容的评审和修订	至少每年一次
中等	逐步浏览计划	会议讨论 IMP、BCP 内容，逐一浏览、讨论计划每个步骤	每年一次
	模拟演练	“虚拟”一个安全事故，相关人员依据 IMP、BCP 进行纸面演练，但不进行实际操作	每年一次或两次
	演练关键活动	只演练一个关键活动，在可控的、不会危及业务正常运作的情形下启动 IMP、BCP 进行演练	每年一次或更低
复杂	全面演练	完全依据 IMP、BCP 进行应急响应，实际启用灾备系统进行业务重续等，验证是否满足 RTO 和 RPO 指标	每年一次或更低

域名服务组织可以根据自己的实际情况、利益相关方的要求，并考虑组织的情况变化和以前演练的结果，灵活安排演练的频次和具体方案。演练的规模和复杂程度应该与组织的业务连续性管理目标相适应。

域名服务组织应制定演练计划，以使因演练直接导致事故的风险最小。演练后应该形成包含建议的总结报告，并根据建议修订相关计划和预案。

10.3 评审

域名服务组织应按计划的时间间隔或在发生重大变化（例如发生事故导致启动BCP或IMP）时，进行业务连续性管理评审，以保证组织的业务连续性能力并与组织实际情况相匹配。评审应有最高管理层参加，评审应确认：

- a) 组织域名服务相关所有关键业务、关键活动及其资源得到了识别；
- b) 组织的BCM方针、策略、响应计划等准确反映了优先级别；
- c) 组织的BCM能力是有效的，达到预期目标，能够有效管理、指挥、控制和协调事故处置；
- d) 组织的BCM方案是有效的，更新及时，达到预期目标，并适合于组织所面临的风险；
- e) 组织的BCM维护和演练方案得到了有效的实施；
- f) BCM策略和计划整合了事故报告、演练报告和方案评审中识别的改进措施；
- g) 组织落实了BCM培训方案；
- h) 组织就BCM方案与相关员工进行了有效沟通，员工理解自身的角色和职责；
- i) 组织设置了BCM变更控制程序，且运行有效。

评审完成后应形成文件化的评审报告，并根据评审结果修订包括BCM方针、BIA结果、BCP文件、IMP文件在内等BCM方案，以保证BCM的持续有效。

10.4 记录和文件管理

域名服务组织在进行业务连续性管理过程中，应对整个业务连续性管理建设和运行过程进行记录，对文件进行版本控制，将记录和文件作为组织内部的知识进行管理，同时也可供主管部门查询。

这些记录和文件包括但不限于业务连续性管理方针文件及其批准记录、业务中断影响分析过程和结果批准记录、风险评估报告和风险处置记录、BCM策略建设方案和过程跟踪记录、事故响应计划（IMP）/业务连续性计划（BCP）/业务恢复计划文件及批准记录、BCM培训/演练/评审记录等。

11 顶级域名注册管理机构要求

11.1 RTO 和 RPO 指标要求

ICANN在对新通用顶级域名申请指南中对顶级域名注册管理机构各项业务的服务级别要求（SLR）（按月衡量）如下。

- a) DNS解析：100%(0中断)。
- b) 域名注册：98%(864min中断)。
- c) 域名查询：98%(864min中断)。

在ICANN的上述最低要求基础上，进一步参考中国国家顶级域名最佳实践，顶级域名注册管理机构各项关键业务和关键活动的RTO和RPO指标应至少满足表5的要求。

表5 RTO 和 RPO 指标要求

域名服务组织	关键业务	关键活动	RTO 指标	RPO 指标
顶级域名注册管理机构	顶级域名解析	Zonefile 文件生成和分发	4h	30min
		DNS 解析	0h	30min
	域名注册	接收域名注册申请	4h	30min
		域名注册审核	24h	24h
	域名查询	WhoisD	4h	30min
		Whois Web	4h	30min

		Whois 批量访问	4h	30min
		可搜索的 Whois	4h	30min
	数据托管	托管数据生成	12h	30min
		托管数据传送给数据托管机构	12h	30min
	财务	注册服务机构续费	24h	30min

11.2 业务连续性管理策略要求

为保证RTO和RPO指标的实现，顶级域名注册管理机构的业务连续性管理策略应满足如下要求：

- a) 顶级域名注册管理机构应充分保证人员和知识的持续可获得，关键业务和关键活动相关的岗位人员应经过充分的技能培训，并实现多人互备。这些人员至少包括系统运行管理人员和域名审核人员。
- b) 顶级域名注册管理机构应有备用工作场所，其中包括备用办公设施。备用办公场所应与主工作场所保持足够的距离。备用工作场所既可以是自有的，也可以与其他机构签署协议由对方应急提供。
- c) 顶级域名注册管理机构应建设同城或异地灾备中心，对关键业务和关键活动所依赖的信息系统和数据进行备份，可以随时进行切换接管服务。关键业务和关键活动所依赖的数据备份的方法和频率应参考8.4节内容，满足对应RPO指标的要求，这些数据包括但不限于域名解析zonefile文件、域名注册数据库数据、域名注册审核材料。
- d) 针对DNS解析系统，顶级域名注册管理机构应实现解析系统的分布式部署，部署5个以上（包括5个）解析节点，并使用任播技术广播解析地址。
- e) 顶级域名注册管理机构关键业务和关键活动所依赖的信息系统应进行充分的冗余，包括多网络链路接入、网络设备和服务器等设备的双/多机热备等，并进行流量负荷分担设计。
- f) 顶级域名注册管理机构应根据政府主管部门和ICANN的要求，利用数据托管服务定期向数据托管机构备份数据。顶级域名注册管理机构应选择由政府主管部门或ICANN认证的、具备资质的数据托管机构，例如ICANN认证的、针对新通用顶级域名注册管理机构和注册服务机构的数据托管代理（Data Escrow Agent）等。

11.3 业务连续性管理响应要求

为保证RTO和RPO指标的实现，顶级域名注册管理机构的业务连续性管理响应工作应满足如下要求。

- a) 顶级域名注册管理机构应建设专门的应急响应组织机构，负责组织和指挥应急响应工作。
- b) 顶级域名注册管理机构应建设专门的应急预案对安全事件的分类、处置流程、处置方法进行规定，遵守政府主管部门要求，在安全事件发生时及时将事件报告给政府主管部门。
- c) 顶级域名注册管理机构应建设专门的业务连续性计划，在灾难情况下启用灾备中心的系统进行业务的重续。关键活动中断时间达到RTO指标的1/2时，顶级域名注册管理机构就应考虑启动业务业务连续性计划。
- d) 顶级域名注册管理机构应与业务接管机构协商建设业务接管方案，在自己的备份措施不能在规定的时间内完成业务重续的情况，由业务接管机构来接管业务，并将其纳入业务连续性计划中。顶级域名注册管理机构应选择由政府主管部门或ICANN认证的、具备资质的业务接管机构，例如ICANN认证的、针对新通用顶级域名注册管理机构和注册服务机构的紧急后台注册管理执行机构（EBERO，Emergency Back-end Registry Operator）等。

e) 顶级域名注册管理机构应至少每年进行一次实战演练，真正启动业务连续性计划，使用灾备中心接管业务并运行一段时间，以验证灾备中心备份系统和备份数据的有效性，保证业务连续性计划的可用。

参 考 文 献

- [1] YD/T 2091-2010 公共域名解析系统安全要求
 - [2] YD/T 2052-2009 域名系统安全防护要求
 - [3] YD/T 2245-2012 域名注册系统安全防护要求
 - [4] GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
 - [5] GB/T 22080:2008/ISO/IEC 27001:2005 信息技术 安全技术 信息安全管理体系 要求
 - [6] BS25999-1:2006 Business Continuity Management. Code of Practice
 - [7] BS25999-2:2007 Specification for Business Continuity Management
-

中华人民共和国
通信行业标准
域名服务业务连续性管理要求
YD/T 2880-2015

*

人民邮电出版社出版发行
北京市丰台区成寿寺路 11 号邮电出版大厦
邮政编码：100164
北京康利胶印厂印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2016 年 2 月第 1 版
印张：1.75 2016 年 2 月北京第 1 次印刷
字数：32 千字

15115 • 791

定价：20 元

本书如有印装质量问题，请与本社联系 电话：(010)81055492