

ICS 35.040

L 80

YD

中华人民共和国通信行业标准

YD/T 2914-2015

信息系统灾难恢复能力评估指标体系

Evaluation index of information system disaster recovery capability

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
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 灾难恢复能力评估方法	1
5 灾难恢复能力评估指标体系	2
5.1 信息系统灾难恢复能力评估指标体系	2
5.2 信息系统灾难恢复体系规划设计能力评估指标域	2
5.3 信息系统灾难恢复体系建设实施能力评估指标域	5
5.4 信息系统灾难恢复体系运行维护能力评估指标域	6

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。

本标准由中国通信标准化协会提出并归口。

主要起草单位：北京邮电大学、中国科学院计算技术研究所、中国信息通信研究院、国防科学技术大学计算机学院。

主要起草人：刘建毅、关继铮、高 翊、王 枫、古 恒、张思悦、宋 震、余宏亮、郑伟民、武永卫、王 飞、杨树强、落红卫。

信息系统灾难恢复能力评估指标体系

1 范围

本标准规定了信息系统灾难恢复能力的评估指标体系。

本标准适用于针对信息系统的灾难恢复服务。

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。

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 20988 信息安全技术 信息系统灾难恢复规范

3 术语和定义

GB/T 20988中界定的以及下列术语和定义适用本文件。

3.1

指标体系 Indicator System

由若干个主要特征定义的指标构成反映该现象本质的系统。

注：指标体系是系统的、具有紧密联系的、反映评价对象整体的一组指标或具体指标的集合。

3.2

灾难恢复体系 Disaster Recovery System

机构为达到其灾难恢复能力所需建立的灾难恢复场地资源、技术资源、人力资源及灾难恢复所需的制度、流程及文档的有机体。

3.3

业务持续计划 Business Continuity Planning

企业在信息系统支持中断的情况下继续经营的能力以及发生灾难性事件情况下的生存能力。

4 灾难恢复能力评估方法

信息系统的灾难恢复体系建设是一项复杂的系统工程，它包括灾难恢复规划和实施、灾难备份中心的日常运行、灾难发生后的应急响应、关键业务功能在灾难备份中心的恢复和重续运行，以及生产系统的灾后重建和回退工作。信息系统灾难恢复体系的建立和维护是一个循序渐进、持续改进、逐步完善的过程。

信息系统灾难恢复能力评估就是对信息系统灾难恢复体系的各个方面进行全面、准确、客观、综合的评估，找出机构灾难恢复体系中存在的缺失和问题，为机构不断改进和完善灾难恢复体系提供帮助。

为使评估工作能覆盖信息系统灾难恢复体系的各个层面和各个角度，需要建立规范化、层次化的评估指标体系以全面反映机构灾难恢复的能力。

5 灾难恢复能力评估指标体系

5.1 信息系统灾难恢复能力评估指标体系

信息系统灾难恢复评估指标体系包括信息系统灾难恢复体系的规划设计能力评估指标域、信息系统灾难恢复体系的建设实施能力评估指标域及信息系统灾难恢复体系运行维护能力评估指标域三个部分。
图 1 为信息系统灾难恢复评估指标体系结构，包括 3 个一级指标项，8 个二级指标项，25 个三级指标项。

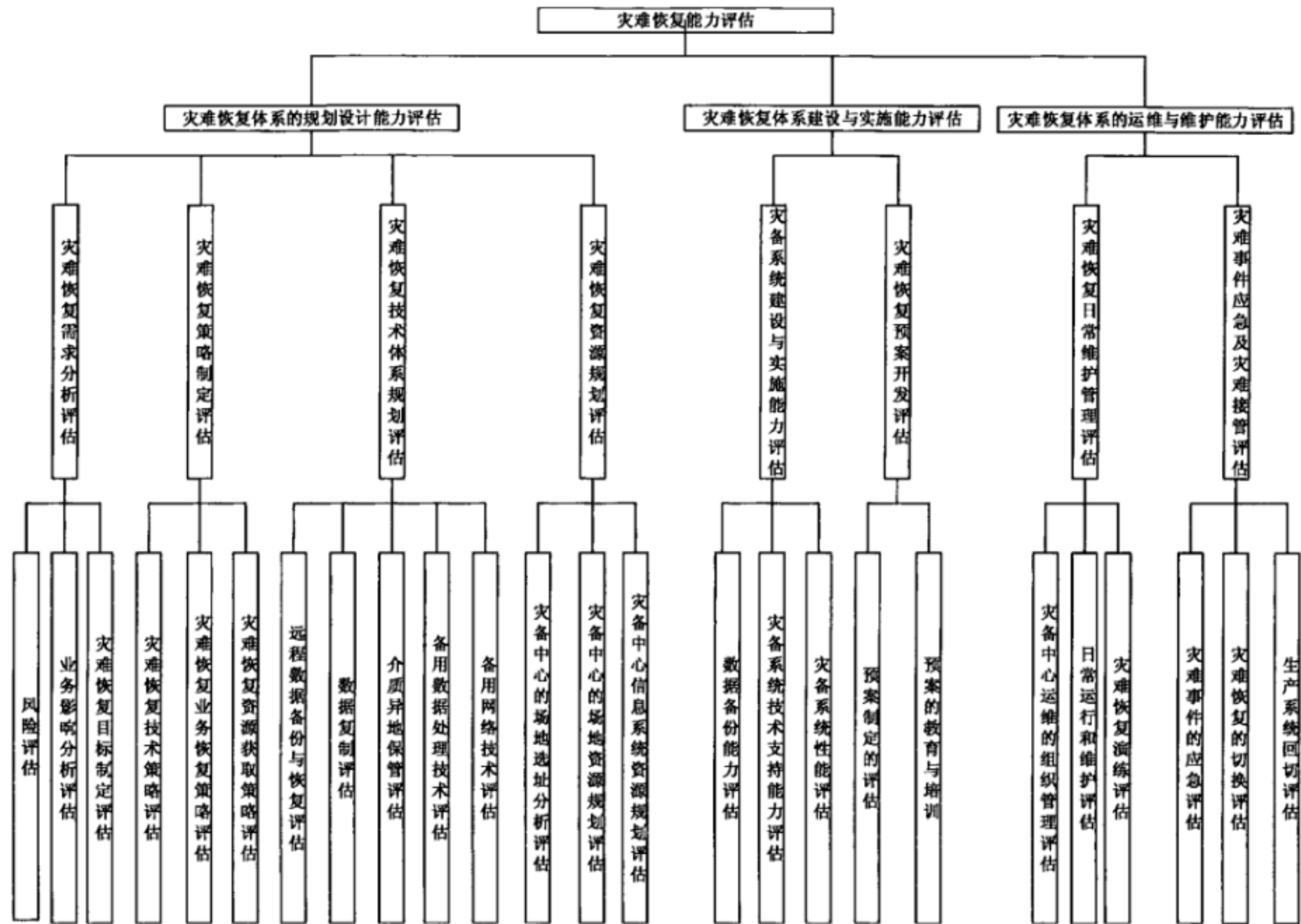


图 1 信息系统灾难恢复能力评估指标

5.2 信息系统灾难恢复体系规划设计能力评估指标域

信息系统灾难恢复体系的规划设计是机构灾难恢复体系的基础性工作，规划设计对灾难恢复体系的建设实施及运行维护起着至关重要的指导作用，灾难恢复体系的规划设计能力集中体现了机构的灾难恢复体系是否满足机构的业务恢复、信息系统恢复的要求，对灾难恢复体系的规划设计能力的评估主要包括灾难恢复的需求分析能力、灾难恢复的策略制定能力、灾难恢复的技术规划能力，以及灾难恢复的资源规划能力。

信息系统灾难恢复体系的规划设计能力评估指标域如表 1 所示。

表1 信息系统灾难恢复体系的规划设计能力评估指标域

1. 信息系统灾难恢复需求分析能力评估指标		
评估指标	指标域	指标域内容
信息系统风险评估能力评估指标	资产识别与评估能力评估	评估机构在信息系统风险评估阶段是否按照GB/T 20984的要求对机构的数据及文档、系统软件、应用软件、源程序、网络设备、计算机设备、存储及备份设备、安全保障设备等资产进行识别与评估

表1 (续)

1. 信息系统灾难恢复需求分析能力评估指标		
信息系统风险评估能力 评估指标	威胁识别与评估	评估机构在信息系统风险评估阶段是否按照GB/T 20984的要求对软硬件故障、物理环境故障、人为误操作、网络攻击、恶意代码、信息泄露等威胁进行识别与评估
	脆弱性识别与评估	评估机构在信息系统风险评估阶段是否按照GB/T 20984的要求对上述相关资产的脆弱性进行识别与评估
	风险分析与管控策略	评估机构在信息系统风险评估阶段是否按照GB/T 20984的要求, 并依据资产、威胁和脆弱性识别与评估分析结果进行了风险计算、风险分析结果判定、风险处理计划的制定和残余风险分析
	信息系统生命周期各阶段的风险评估	评估机构在信息系统的规划设计、建设实施及运行维护等阶段进行的风险评估是否符合GB/T 20984的要求
	风险评估文档管理	对机构的风险评估文档管理的规范性进行评估
数据中心基础设施风险评估	服务商评估	对数据中心基础设施服务商的资质及能力进行评估
	资产识别及赋值	评估机构在数据中心基础设施风险评估中是否按照规范的要求对数据中心的建筑构造和物理环境所涉及的资产进行了识别和评估
	威胁识别与评估	评估机构在数据中心基础设施风险评估中是否按照规范的要求对数据中心的建筑构造和物理环境所面临的威胁进行了识别和评估
	脆弱性识别与评估	评估机构在数据中心基础设施风险评估中是否按照规范的要求对数据中心的建筑构造和物理环境脆弱性进行了识别和评估
	风险分析与管控策略	评估机构的风险评估结论、处理计划和残余风险分析是否满足规范的要求, 是否按照上述的资产、威胁和脆弱性识别与评估结果得出的结论
业务影响分析	关联性分析	评估机构在业务影响分析中是否进行了业务的关联性分析, 在关联性分析中是否综合考虑了机构的业务功能、业务之间的关联性、业务与信息系统的关联性, 以及信息系统之间的关联性
	业务中断影响分析	评估机构在业务影响分析中是否进行了业务中断影响分析, 在业务中断影响分析中是否与业务部门进行充分沟通, 并对业务的中断时间、中断后造成的财务和非财务影响进行了全面的分析
	灾难恢复优先级别确立	评估机构在业务影响分析中是否进行了灾难恢复优先级别的分析 and 确立, 灾难恢复优先级别的分析方法是否规范, 分析结果是否得到相关部门的确认
	灾难恢复指标确立	评估机构在业务影响分析中所确立的灾难恢复指标是否按照业务中断影响分析的结论并得到相关部门的确认
灾难恢复目标的制定	灾难恢复等级制定	评估机构所确立的灾难恢复范围和灾难恢复等级是否机构灾难恢复指标和优先级别的要求
	灾难恢复资源需求	评估机构是否按照GB/T 20988的要求确立对应灾难恢复等级的资源需求

表1 (续)

2. 信息系统灾难恢复策略分析能力评估指标		
评估指标	指标域	指标域内容
灾难恢复技术策略	数据备份策略	评估机构所制定的数据备份方式、流程和验证机制
	数据复制策略	评估机构的数据复制策略是否满足复制要求
	系统切换策略	评估机构的系统切换策略是否满足系统切换和接管要求
业务恢复策略	数据追补策略	评估机构的数据追补策略是否能在生产端数据丢失时进行追补
	手工替代恢复业务策略	评估机构的手工替代方式是否满足业务恢复的要求
	业务恢复优先顺序	评估机构的业务恢复优先顺序是否满足业务恢复的要求
	业务恢复流程	评估机构的业务恢复流程是否满足业务恢复的要求
	业务恢复人员及岗位职责	评估机构的业务人员及岗位职责是否能在灾难发生时完成业务恢复
灾难恢复资源获取策略	灾难备份中心资源获取策略	评估机构的灾难备份中心资源获取策略是否经过了科学论证, 并符合机构的投资方式
	灾难备份系统资源获取策略	评估机构的灾难备份系统资源获取策略是否经过了科学论证, 并符合机构的投资方式
	灾难备份中心人力资源获取策略	评估机构的人力资源获取策略是否具备可操作性
	灾难备份中心配套设施获取策略	评估机构的配套资源获取策略是否满足灾难备份中心配套设施要求
3. 灾难恢复技术体系规划评估指标域		
评估指标	指标域	指标域内容
远程数据备份与恢复	备份与恢复需求	评估机构的备份与恢复需求是否全面
	备份与恢复技术	评估机构的备份与恢复技术是否具备可操作性
实时数据复制	复制方式	评估机构的数据复制方式是否满足灾难恢复指标的要求
	复制层次	评估机构的数据复制层次是否满足数据复制策略的要求
介质异地保管	存储介质	评估机构的备用存储介质是否满足数据恢复验证的要求
	介质异地转储制度	评估机构的介质转储制度是否满足异地介质管理要求
备用数据处理技术	备用数据处理平台的部署规划	评估机构的备用数据处理平台部署规划是否满足关键业务接管要求
	应用系统的部署	评估机构的应用系统部署规划是否满足数据处理平台部署规划及关键业务接管要求
	生产与灾备系统的切换与回切技术	评估机构的切换与回切技术是否满足关键业务系统接管要求
备用网络技术	灾备中心的网络平台部署	评估机构的网络平台部署规划是否满足应用系统部署要求
	生产与灾备网络系统的切换与回切技术	评估机构的网络切换与回切技术是否满足应用系统切换要求
	灾备中心与关联渠道的网络互连技术	评估机构的网络互连技术是否满足切换到灾难备份中心后的渠道交易需求

表1 (续)

4. 灾难恢复资源规划评估指标域		
评估指标	指标域	指标域内容
灾备中心的人力资源管理规划评估指标域	灾备规划人员组织结构和分工	评估机构的灾难恢复规划人员是否满足灾难恢复规划的要求
	灾备实施人员组织结构和分工	评估机构的灾难备份系统实施人员是否满足灾难备份系统实施的要求
	灾备系统规划与实施人员的培训	评估机构的人员培训是否满足灾难备份系统规划和实施的技能要求
灾备中心的场地选址分析评估指标域	场地需求分析	评估机构的灾难备份中心场地需求是否符合相关标准和监管机构的要求, 是否符合机构灾难恢复的要求
	选址指标	评估机构的灾难备份中心选址是否具有科学性
灾备中心的场地资源规划	灾备中心的园区及建筑物规划	评估机构的灾难备份中心园区及建筑物规划是否全面
	灾备中心的基础设施规划	评估机构的灾难备份中心基础设施规划是否全面
	灾备中心的场地布局规划	评估机构的灾难备份中心场地布局规划是否合理
灾备中心信息系统资源规划	数据容量规划	评估机构的灾难备份中心的数据容量是否满足灾难恢复数据容量要求
	处理能力规划	评估机构的灾难备份中心的处理能力是否满足灾难备份系统接管生产能力要求
	网络资源配置规划	评估机构的灾难备份中心的网络资源是否满足系统切换和灾备端交易的要求
	灾备中心安全管理规划	评估机构的灾难备份中心的安全管理是否满足灾难备份系统稳定运行的要求

5.3 信息系统灾难恢复体系建设实施能力评估指标域

信息系统灾难恢复体系的建设实施是机构依据灾难恢复体系规划设计要求进行灾难恢复体系建设, 包括灾难备份信息系统建设及灾难恢复预案体系建设, 灾难恢复体系的建设实施能力集中体现数据备份能力、技术支持能力、灾难备份系统运行和验证能力、灾难恢复预案的开发能力。

信息系统灾难恢复体系的建设实施能力评估指标域如表2所示。

表2 信息系统灾难恢复体系的建设实施能力评估指标域

1. 灾难备份系统建设实施能力评估指标域		
评估指标	指标域	指标域内容
数据备份能力	备份数据的一致性和完整性	评估机构的数据验证机制是否真正落实
	备份数据的可用性	评估机构的备份数据可用性验证是否全面
	复制数据的可用性	评估机构的复制数据可用性验证是否全面
灾备系统技术支持能力	实施人员的技术能力	评估机构的实施人员是否满足灾难备份技术实施所需的技能要求
	技术管理流程和制度	评估机构的技术管理体系是否能保证灾难备份系统实施要求
	知识体系的可用性和完备性	评估机构的灾难备份系统实施知识体系的完备性
灾备系统性能	业务层面的灾备指标满足度	评估机构的灾难备份系统是否满足业务层面灾难恢复指标
	信息系统层面的灾备指标满足度	评估机构的灾难备份系统是否满足信息系统层面灾难恢复指标

表2 (续)

2. 灾难恢复预案开发能力评估指标域		
评估指标	指标域	指标域内容
预案的制定	总案及应急管理规范	评估机构所开发的总案及应急管理规范的完备性
	基于灾难场景的专项预案	评估机构的场景预案的完备性
预案的教育与培训	预案的教育与培训	评估机构的预案培训和教育体系是否有利于预案在机构的宣教和贯彻

5.4 信息系统灾难恢复体系运行维护能力评估指标域

信息系统灾难恢复体系的运行维护是机构依据灾难恢复体系规划设计要求进行灾难备份体系的运行维护,灾难恢复体系的运行维护能力集中体现在日常运维和突发事件应急及灾难恢复两个方面。

信息系统灾难恢复体系的运行维护能力评估指标域如表3所示。

表3 信息系统灾难恢复体系的运行维护能力评估指标域

1. 灾难恢复体系的日常维护管理指标域		
评估指标	指标域	指标域内容
灾备中心运维的组织管理	运维人员的组织架构和岗位职责	评估机构的灾难备份中心运维组织架构是否满足日常运维管理的要求
	运维团队的沟通和协调机制	评估机构的灾难备份中心运维团队的沟通协调机制是否有利于提升日常运维管理的效率
日常运行和维护	基准核对	评估机构的生产与灾备的基准文档及日常的基准核对机制
	子系统的切换验证	评估机构的生产与灾备的子系统切换是否有效
	灾备系统的可用性验证	评估机构的灾难备份系统的可用性验证是否满足灾备系统接替生产运行的要求
预案管理	保存与分发	评估机构的灾难恢复预案的保存与分发是否满足预案管理要求
	维护与变更	评估机构的灾难恢复预案的维护与变更是否满足预案管理要求
灾难恢复演练	演练的准备	评估机构灾难恢复演练的准备工作是否完善、周到
	演练的培训	评估机构是否对相关人员进行演练培训
	演练的技术支持	评估机构的演练技术支持工作是否完善
	演练的切换与回退	评估机构的演练切换与回退流程是否完善
	演练过程中突发事件的应急处置	评估机构是否有对演练过程中的突发事件应急处置手段
	演练的回顾与总结	评估机构是否有对演练过程中的分析总结
2. 突发事件应急与灾难接管能力评估指标域		
评估指标	指标域	指标域内容
突发事件的应急	灾难的预警、宣告流程	评估机构的灾难发生时的预警和宣告机制是否有效
	灾难发生时的损失控制和协调机制	评估机构是否有灾难发生时的损失控制和协调机制
	系统监控与验证	评估机构是否有灾难发生时的系统监控与验证能力
灾难恢复的切换	系统和数据的恢复	评估机构灾难发生时系统和数据恢复能力
	业务功能的恢复	评估机构灾难发生时业务功能恢复能力
	灾备系统接替生产运行	评估机构灾难发生时系统接管能力
生产系统回切	灾难发生后的损害评估	评估机构是否有灾难发生后的损害评估
	灾备系统回切及生产系统重续运行	评估机构灾难发生时的系统回切及重续运行能力

中华人民共和国
通信行业标准
信息系统灾难恢复能力评估指标体系
YD/T 2914-2015

*

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 2015年12月第1版
印张：0.75 2015年12月北京第1次印刷
字数：18千字

15115·833

定价：10元

本书如有印装质量问题，请与本社联系 电话：(010)81055492