ICS 35.030
CCS L 80

团　　体　　标　　准

T/CIIPA 00013—2024

自主可控网络安全技术　云灾备平台功能要求

Autonomous and controllable cybersecurity technology—Functional requirements for cloud disaster recovery platform

全国团体标准信息平台

2025-06-09 发布　　2025-06-11 实施

中关村华安关键信息基础设施安全保护联盟　发布
中　国　标　准　出　版　社　出版

目　　次

前言 ……Ⅲ
引言 ……Ⅳ
1　范围 ……1
2　规范性引用文件 ……1
3　术语和定义 ……1
4　缩略语 ……3
5　通则 ……3
6　基本功能要求 ……3
6.1　资源管理……3
6.2　备份与恢复……4
6.3　用户管理……5
6.4　鉴别认证……5
6.5　监控告警……6
6.6　安全审计……6
7　拓展功能要求 ……6
7.1　数据传输……6
7.2　数据存取……7
7.3　数据销毁……7
附录 A（资料性）　业务重要程度分类标准与灾难恢复能力等级指标对应关系表 ……8
附录 B（资料性）　业务连续性要求分级标准与灾难恢复能力等级指标对应关系表……9
附录 C（资料性）　容灾备份服务类型与灾难恢复能力等级指标对应关系表 ……11
参考文献 ……12

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由中关村华安关键信息基础设施安全保护联盟提出并归口。

本文件起草单位：奇安信科技集团股份有限公司、北方工业大学、北京邮电大学、北京信息灾备技术产业联盟、北京国腾创新科技有限公司、深圳云安宝科技有限公司、柏科数据技术（深圳）股份有限公司、上海交通大学、北京中嘉和信通信技术有限公司、迪思杰（北京）数据管理技术有限公司、工业和信息化部电子第五研究所、北京柏睿数据技术股份有限公司、浙江脑动极光医疗科技有限公司。

本文件主要起草人：吴云坤、马礼、纪胜龙、杨光灿、何云华、邱浩、成国强、刘浩、姚磊、张春勇、江雯雯、高超、陈蔚、王颖、王晓怡、云雷、腾迪、赵菁华、王思登、张坤、蔡龙军、李芳、杨晓平、游录金、吴晨涛、梁军海、佟淑杰、闫包三、王伟红。

全国团体标准信息平台

引　言

保障关键信息基础设施安全的一个很重要方面是保障关键信息基础设施的业务连续性，确保关键数据和系统在遭遇灾难时能够迅速恢复和业务的不间断运行，对关键信息基础设施的正常运行至关重要。云计算和云存储等相关技术的发展为云灾备的广泛应用奠定了坚实的基础，为数据的容灾和备份带来了诸多便利。云灾备的应用可以在灾难发生后快速、准确地恢复业务数据和关键应用系统，保障业务的连续运行，进一步降低企业的信息化成本。作为云灾备服务的主要产品，云灾备平台的自主可控程度直接关乎“信息安全保障最后一道防线”的安全能力。因此，制定具有自主可控“基因”的云灾备平台功能要求是十分必要的，有利于引领信息灾备产品研发和使用过程中自主、安全、可控意识的提升，促进信息灾备产业的健康发展。

全国团体标准信息平台

自主可控网络安全技术　云灾备平台
功能要求

1　范围

本文件主要规定了自主可控云灾备平台所需提供的基本功能和拓展功能要求。

本文件适用于国产云灾备平台功能的设计、研发和建设等。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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。

GM/T 0002　SM4 分组密码算法

GM/T 0003　SM2 椭圆曲线公钥密码算法

GM/T 0004　SM3 密码杂凑算法

GB/T 20988　信息安全技术　信息系统灾难恢复规范

GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求

GB/T 25069—2022　信息安全技术　术语

GB/T 29765—2021　信息安全技术　数据备份与恢复产品技术要求与测试评价方法

GB/T 32400—2015　信息技术　云计算　概览与词汇

T/ZISIA 01—2024　自主创新型网络安全技术　框架

3　术语和定义

GB/T 25069—2022 和 GB/T 32400—2015 中界定的下列术语和定义适用于本文件。

3.1

云灾备　cloud disaster recovery

对承载的业务系统和数据进行基于云存储的备份,并在必要时能够实施可靠性恢复的模式。

3.2

云灾备平台　cloud disaster recovery platform

以云存储为容灾基础,实施备份和恢复的软件或系统。

3.3

用户　user

基于云灾备平台实现灾难备份的数据所有方。

3.4

灾难备份　disaster backup

为了灾难恢复而对数据、数据处理系统、基础设施、专业技术支持能力和运行管理能力进行备份的过程。

3.5

实例信息　instance information

用户对备份计划和恢复任务进行实例化的状态信息。

3.6

完全备份　trusted full backup

备份所有指定的数据对象的过程，不论这些数据自上次备份后是否被更改。

[来源：GB/T 29765—2021，3.9]

3.7

增量备份 incremental backup

仅备份自上次备份后更改过的数据对象的过程。

[来源：GB/T 29765—2021，3.10]

3.8

保密性　confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的性质。

[来源：GB/T 25069—2022，3.41]

3.9

完整性 integrity

准确和完备的性质。

[来源：GB/T 29246—2023，3.36]

3.10

备份对象　backup object

需要进行备份的数据集合。

[来源：GB/T 29765—2021，3.5]

3.11

可用区　availability zone

在云灾备服务中，综合考虑电力、网络、供水等基础设施作为独立容灾因素划分出来的物理区域，区域内包含空调、电力设施、主机、网络、存储等容灾物理资源。

3.12

恢复点目标　recovery point objective

为使活动能够恢复操作而需将其所用信息恢复的时间点。

[来源：GB/T 25069—2022，3.253]

3.13

恢复时间目标　recovery time objective

从时间发生到完成恢复产品或服务、活动或者资源之间的时间段。

[来源：GB/T 25069—2022，3.254]

3.14

网络恢复目标　network recovery objective

灾难发生后，到备用网络系统所需的时间。

3.15

任意时间点回退　any point in time

能够将数据恢复到过去任何一个具体的时间点的历史状态。

4 缩略语

下列缩略语适用于本文件。

UID:用户标识符(User Identifier)

API:应用程序编程接口(Application Programming Interface)

CPU:中央处理器(Central Processing Unit)

RTO:恢复时间目标(Recovery Time Objective)

RPO:恢复点目标(Recovery Point Objective)

NRO:网络恢复目标(Network Recovery Objective)

APIT:任意时间点回退 (Any Point In Time)

5 通则

云灾备平台能够对业务数据和关键应用系统进行备份和恢复,是确保数据安全性和可靠性以及保障业务连续性的重要手段。自主可控的云灾备平台是网络安全的重要组成部分,能够有效应对网络攻击,保护关键信息基础设施。根据备份和恢复资源是否跨可用区,自主可控云灾备平台的功能要求有所不同。在不涉及备份和恢复资源跨可用区的应用场景下,自主可控云灾备平台应满足基本功能要求,在基本功能要求中,资源管理、备份与恢复属于平台的自身功能要求,而用户管理、鉴别认证、监控告警和安全审计属于平台的安全功能要求;在涉及备份和恢复资源跨可用区的应用场景,自主可控云灾备平台除满足基本功能要求之外,还应满足拓展功能要求。自主可控的云灾备平台功能要求具体如表 1 所示。

表 1 自主可控云灾备平台功能要求

功能要求	资源管理	备份与恢复	用户管理	鉴别认证	监控告警	安全审计	数据传输	数据存取	数据销毁
基本功能要求	√	√	√	√	√	√			
拓展功能要求							√	√	√

6 基本功能要求

6.1 资源管理

6.1.1 资源统计

云灾备平台应支持对服务器类资源,存储类资源,网络类资源、虚拟机类资源和软件类资源等各类资源信息的统计,实现的资源统计功能包括但不限于:

a) 应支持对各类资源使用情况的统计,如对虚拟机类资源和网络类资源的资源总量及使用程度的统计;

b) 应支持对所有用户使用的现有资源成本及历史资源成本等情况的统计,如对用户数量、资源分配情况、服务资源占用率等信息的统计;

c) 应支持以用户为单位统计实例信息,并支持实例状态展示,如实例名称、实例创建时间、实例执行状态和实例启动时间等;

d） 应支持以用户为单位统计实例资源使用情况，如实例数量、实例资源分配等信息，并支持统计结果展示，如用户可按照统计项（如实例创建时间）进行排序，按照分页浏览模式进行查看；

e） 应支持以角色和权限的信息统计和展示，如根据登录用户的角色和权限进行相应统计结果的展示，对没有权限查看的统计结果不进行展示；

f） 应支持对统计结果的图形化展示，展示图形包括常见的饼状图和柱状图等。

6.1.2 资源记录

云灾备平台应支持记录服务器类资源，存储类资源，网络类资源、虚拟机类资源和软件类资源等各类资源数量的历史信息及其当前的基本信息，实现的资源记录功能包括但不限于：

a） 应支持记录各类资源的历史使用情况，如每类资源的总量及占用情况；

b） 应支持以用户为单位对资源使用的历史情况进行记录；

c） 应支持对实例信息的创建、启动、暂停、修改和删除等关键操作的记录；

d） 应支持对实例使用情况和实例资源使用情况的历史记录，以及以用户为单位的实例资源使用情况记录；

e） 应支持与资源管理交互产生的历史日志记录；

f） 应支持备份和恢复过程中的出错处理记录；

g） 应支持历史日志的导出功能，导出的历史日志为常见文件格式类型。

6.2 备份与恢复

6.2.1 备份对象

应支持在国产化软硬件平台上进行备份和恢复操作，涉及的对象包括但不限于：

a） 应支持对国产文件系统及其数据、结构和状态进行备份和恢复；

b） 应支持对国产操作系统及其数据、结构进行备份和恢复；

c） 应支持对基于国产化 CPU 架构的物理机和虚拟机进行备份和恢复；

d） 应支持对国产数据库管理系统及其数据、结构和状态进行备份和恢复。

6.2.2 备份方式

应支持灵活可控的备份和恢复方式，所应具备的方式包括但不限于：

a） 应支持完全备份和增量备份等方式；

b） 应支持实时和定时的备份和恢复方式；

c） 应支持手动和自动可切换的备份和恢复方式。

6.2.3 灾难恢复

根据 T/ZISIA 01—2024 关于能够依据业务重要性进行备份和恢复的规划和实施的要求，云灾备平台应满足不同业务重要程度、不同业务连续性要求和不同灾难恢复策略情况下的灾难恢复能力等级要求，以确保关键业务能够得到适当的保障和恢复，并足以支撑起相应的灾难恢复策略。RTO 对应业务不可用的时间长度，即在多长时间内需要恢复业务的正常运行。RPO 对应业务丢失的数据，即在灾难发生前多久的业务数据状态需要被恢复。

a） 业务重要程度。

云灾备平台的灾难恢复能力等级应满足其能够支撑的业务重要程度，业务重要程度的分类依据可参考 GB/T 22240—2020 对于等级保护对象的规定，分析维度包括但不限于：利益影响范围，经济损失程度，人员影响范围等。根据业务重要程度的分析结论，将云灾备平台支持的业务重要程度分为五类，

对应的灾难恢复能力等级指标 RTO 和 RPO 指标参见附录 A 的 A.1。

b） 业务连续性要求。

云灾备平台的灾难恢复能力等级应满足其能够支撑的业务连续性要求，业务连续性要求分级依据的分析维度包括但不限于：业务核心功能，业务间依赖程度、业务中断影响等。其中，业务核心功能的分析范围包括但不限于：机构服务目标，关键流程识别和机构核心价值等；业务间依赖程度的分析范围包括但不限于：业务数据流，业务基础架构和关键资源模块等；业务中断影响的分析应根据 GB/T 20988 规定的方法，对业务功能的中断造成的影响进行评估。根据业务连续性要求的分析结论，将云灾备平台支持的业务连续性要求分为五级，对应的灾难恢复能力等级指标 NRO 和 APIT 指标参见附录 B 的 B.1。

c） 灾难恢复策略。

云灾备平台的灾难恢复能力等级应满足其能够支撑的灾难恢复策略，不同的灾难恢复策略应符合不同的业务连续性要求，根据云灾备平台能够支撑的业务连续性要求，对应灾难恢复能力等级指标 RTO 和 RPO 指标参见 B.2。此外，不同的灾难恢复策略应符合不同的容灾备份服务类型，根据云灾备平台能够支撑的容灾备份服务类型，对应灾难恢复能力等级指标 RTO 和 RPO 指标参见附录 C 的 C.1。

6.3 用户管理

云灾备平台应支持用户注册、登录、口令修改、注销等操作，以及管理员对角色和权限的分配等管理功能，用户管理功能包括但不限于：

a） 应支持用户进行注册和信息录入；

b） 应支持用户对其注册和录入信息进行修改，关键信息（如唯一用于身份鉴别和认证的 UID 信息）可设置为不可修改；

c） 应支持使用国产商用密码算法对用户口令进行加密存储和完整性校验的方法，保障口令的保密性和完整性；

d） 应支持用户进行口令修改。更改口令时，用户需要提交原口令、新口令和确认新口令等验证信息，验证结果成功或失败，都需对用户进行反馈；

e） 应支持用户进行口令重置，口令重置需要用户提供能够鉴别其身份的信息，如身份鉴别信息核对成功，向用户反馈重置后的链接，如身份鉴别信息核对失败，向用户反馈失败原因；

f） 应支持用户进行注销，完成用户使用资源的释放和用户数据的清理；

g） 应支持用户状态管理，如挂起和冻结操作，并暂停用户所有资源的使用；

h） 应支持角色管理，包括管理员对用户赋予/取消角色，以及对角色的创建、修改、查询和删除等操作；

i） 应支持权限管理，如管理员对用户不同角色分配不同的操作权限，以及对角色进行权限的增加、修改和删除等操作；

j） 应支持对每个用户创建独立且隔离的存储空间，除授权用户外，存储空间不可改、不可读。

6.4 鉴别认证

云灾备平台应符合 GB/T 22239—2019 中对于身份鉴别的要求，支持对一般用户和系统用户（如系统管理员）进行身份标识与鉴别，以及登录合法性认证，实现的鉴别认证功能包括但不限于：

a） 应以用户名和 UID 等信息对用户进行标识，且 UID 具有唯一性；

b） 应支持基于国产商用密码算法进行身份鉴别的方式；

c） 应支持身份鉴别错误限制机制，并可预先规定错误尝试次数上限和鉴别失败的安全处理措施；

d） 应支持超时锁定机制，超时后需重新进行身份鉴别；

e） 应支持加盐散列的身份认证方式，且应使用国产散列算法进行加盐散列值的计算；

f） 应支持口令周期更换的审查功能，且更换周期的提示不多于 90 d。

6.5 监控告警

云灾备平台应支持 API 等方式对服务器类资源，存储类资源，网络类资源、虚拟机类资源和软件类资源等各类资源进行监测和告警，实现的监测告警功能包括但不限于：

a） 应支持对各类资源的运行状态和空间使用情况进行监测和展示；
b） 应支持告警及告警处理机制，如对各类资源的异常告警、备份失败告警、恢复失败告警和快照失败告警等告警信息的收集，并根据预先定义的告警处理机制，将告警信息通知相关人员，进行及时处理；
c） 应支持对各类资源告警规则的自定义功能，告警规则如告警类型、告警级别和告警阈值等；
d） 应支持对各类资源告警规则的创建和管理功能，以及告警记录的查询和显示功能；
e） 应支持对各类资源的告警确认功能，可配置自动确认开关，对非重要告警支持系统自动确认。

6.6 安全审计

应符合 GB/T 29765—2021 中 6.2.3 所规定的安全审计要求，执行定期安全审计机制和受保护的审计信息存储，支持的审计功能包括但不限于：

a） 应支持对系统管理员的重要操作如分配和变更用户权限等行为进行详情记录，并能够对可能的违规行为提供问责证据；
b） 应支持对用户的异常操作如登录尝试等行为进行详情记录，确保相关事件都被记录并可供后续分析和审计；
c） 应具有相关措施防止审计进程未经授权的中断，确保行为事件的真实性；
d） 应支持使用国产商用密码算法对被审计信息进行完整性保护，保障审计的行为事件记录不被篡改，保障行为事件的完整性审计；
e） 应支持对用户的业务资源使用情况如资源操作行为的操作日期、操作对象和操作内容等进行记录，提供可能的追溯证据；
f） 应支持使用国产商用密码算法对备份前数据进行完整性校验的措施；
g） 审计日志的留存时间不应少于 6 个月。

7 拓展功能要求

7.1 数据传输

应支持在不同可用区之间的数据传输，所应具备的数据传输安全功能包括但不限于：

a） 应支持对备份和恢复的两端主体执行基于国产商用密码算法（符合 GM/T 0002、GM/T 0003 和 GM/T 0004 等）的身份鉴别和认证，验证其身份的真实性和合法性；
b） 应满足数据传输安全的保密性策略以及相应的安全控制措施，如支持基于国产商用密码算法进行的数据加密和安全信道的构建等；
c） 应支持对数据传输接口进行安全管理，如对可用区之间数据传输接口的安全管理；
d） 应支持对传输数据进行完整性校验的安全控制措施，如基于国产商用密码算法构建的消息认证码；
e） 应支持对数据传输安全策略的变更进行审核和监控，包括通道安全配置、密码算法配置、密钥管理和一键更新密钥等安全策略。

7.2 数据存取

应支持在不同可用区之间的数据存储，所应具备的数据存储安全功能包括但不限于：

a） 应支持开放可伸缩数据存储架构，满足数据量持续增长的存储需求；

b） 应支持对存储数据的相关安全操作，如访问控制、存储转移、数据一致性检测等；

c） 应支持基于国产商用密码算法如 GM/T 0002、GM/T 0003 和 GM/T 0004 等的数据加解密处理和密钥管理；

d） 应支持对重要数据进行加密存储并具备防止篡改的措施；

e） 应支持对数据存储介质的标识，标识应具备明确的命名规则和标识属性等重要信息，并定期验证数据的完整性和可用性；

f） 应支持多用户数据的存储安全隔离，不同用户间的数据不可以相互访问。

7.3 数据销毁

应支持跨可用区的数据安全销毁，所应具备的数据销毁安全功能包括但不限于：

a） 应以不可逆方式销毁备份数据，确保销毁后的数据无法恢复和正常使用；

b） 应支持对销毁数据的审批和监管，明确销毁对象、销毁流程、销毁方式和销毁要求。

全国团体标准信息平台

附 录 A
（资料性）
业务重要程度分类标准与灾难恢复能力等级指标对应关系表

A.1 业务重要程度分类标准与RTO/RPO对应关系表

表A.1说明了业务重要程度分类与RTO/RPO的对应关系。

表A.1 业务重要程度分类与RTO/RPO的对应关系表

业务重要程度分类	分类描述	RTO	RPO
第一类	涉及国家安全、社会秩序、经济建设及公共利益的关键业务，在遭遇短暂中断或数据丢失时，将对社会秩序、经济建设和公共利益产生严重冲击，对相关职能领域、机构资产和人员造成极端严重的负面效应	≤5 min	0
第二类	涉及国家安全、社会秩序、经济建设以及公共利益的关键业务，在遭遇短期中断或数据丢失的情况下，对社会秩序、经济建设和公共利益产生显著的不利影响，对于公民、法人及其他组织的合法权益带来较大的冲击，对相关职能领域、机构资产及工作人员产生严重的负面效应	≤15 min	0
第三类	涉及国家安全、社会秩序、经济建设以及公共利益的一般业务，在遭遇短期中断或数据丢失的情况下，对日常服务、职能履行、公民日常生活产生一定影响，对于相关职能领域、机构资产、机构形象和声誉造成较大的负面影响	≤12 h	≤12 h
第四类	涉及处理重要信息和提供重要服务的业务，在遭遇短期中断或数据丢失的情况下，对于相关职能领域、机构资产、机构形象和声誉造成一般的负面影响	≤24 h	≤24 h
第五类	涉及处理一般信息和提供一般服务的业务，在遭遇短期中断或数据丢失的情况下，对于相关职能领域、机构资产、机构形象和声誉造成较小或基本不产生负面影响	≤2 d	≤48 h

附 录 B
（资料性）
业务连续性要求分级标准与灾难恢复能力等级指标对应关系表

B.1 业务连续性要求分级标准与NRO/APIT对应关系表

表 B.1 说明了业务连续性要求分级标准与 NRO/APIT 的对应关系。

表 B.1 业务连续性要求分级标准与 NRO/APIT 的对应关系表

业务连续性要求分级	描述	NRO	APIT
核心级	直接关系到机构的核心功能和服务目标	秒级	毫秒级
	对其他业务有着决定性的影响，如果出现问题，会导致整个机构运营受到严重影响		
	业务中断会对机构造成极其严重的负面影响		
重要级	支持核心级业务功能的重要业务	分钟级	秒级
	对机构的正常运作起着重要的支持作用，如果出现问题，会对核心业务产生一定的影响		
	业务中断会对机构造成严重的负面影响		
一般级	支持日常运营的常规性业务	≤12 h	分钟级
	对机构的正常运作有一定的影响，如果出现问题，不会对核心业务造成直接的影响		
	业务中断会对机构造成较大的负面影响		
辅助级	非关键性的辅助性业务	≤24 h	小时级
	如果出现中断等问题，也不会对核心业务造成影响		
	业务中断会对机构造成一定的负面影响		
建议级	探索性、实验性或临时性的业务	≤2 d	天级
	如果出现中断等问题，也不会对其他业务造成影响		
	业务中断会对机构造成较小的负面影响		

B.2 业务连续性要求分级标准与RTO/RPO对应关系表

表 B.2 说明了业务连续性要求分级标准与 RTO/RPO 的对应关系。

表 B.2 业务连续性要求分级标准与 RTO/RPO 的对应关系表

业务连续性要求分级	RTO	RPO
核心级	RTO≤5 min	RPO=0
重要级	RTO≤15 min	RPO=0
一般级	RTO≤12 h	RPO≤12 h

表 B.2　业务连续性要求分级标准与 RTO/RPO 的对应关系表（续）

业务连续性要求分级	RTO	RPO
辅助级	RTO≤24 h	RPO≤24 h
建议级	RTO≤2 d	RPO≤48 h

全国团体标准信息平台

附 录 C
（资料性）
容灾备份服务类型与灾难恢复能力等级指标对应关系表

C.1 容灾备份服务类型与RTO/RPO对应关系表

表C.1说明了容灾备份服务类型与RTO/RPO的对应关系。

表C.1 容灾备份服务类型与RTO/RPO的对应关系表

容灾备份服务类型	应用场景描述	RTO	RPO
同可用区云容灾备份服务	在云端部署备份业务系统，通过启动云端备份业务系统提供同可用区之间的云灾备服务	分钟级	天级
非同可用区云容灾备份服务	在云端部署备份业务系统，通过启动云端备份业务系统提供非同可用区之间的云灾备服务	分钟级	小时级
多可用区云容灾备份服务	在至少有一个非同可用区的云端部署两套或者多套备份业务系统，通过启动云端备份业务系统可以同时提供云灾备服务	分钟级	分钟级

全国团体标准信息平台

参 考 文 献

[1] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
[2] GB/T 29246—2023 信息技术 安全技术 信息安全管理体系 概述和词汇

全国团体标准信息平台