ICS 03.060
A 11

IAC

中 国 保 险 行 业 协 会 标 准

T/IAC 8—2017

保险业公有云资源管理基本要求

Basic requirement for cloud resource management in insurance industry

2017-12-29 发布　　2018-06-12 实施

中国保险行业协会　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中国保险行业协会提出并归口。

本标准起草单位：阳光保险集团股份有限公司、中国太平洋保险（集团）股份有限公司、中国人民保险集团股份有限公司、信美人寿相互保险社。

本标准主要起草人：高建、姚琦、李波、顾睿、袁娟、王博。

保险业公有云资源管理基本要求

1 范围

本标准规定了保险业使用公有云资源的基本要求、安全管理、资源管理、数据管理和应急管理与培训等相关内容。

本标准适用于保险业使用公有云相关的基本要求、安全管理、资源管理、数据管理和应急管理与培训等，本标准不适用于保险业使用的私有云资源。

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。

ISO/IEC 20000-1:2011 信息技术 服务管理 第1部分:服务管理体系要求(Information technology—Service management—Part 1:Service management system requirements

ISO/IEC 20000-2:2012 信息技术 服务管理 第2部分:服务管理系统的应用指南(Information technology—Service management—Part 2:Guidance on the application of service management systems)

ISO/IEC 22301:2012 社会安全 营运管理体系 要求(Societal security—Business continuity management systems—Requirements)

ISO/IEC 27001:2013 信息技术 安全技术 信息安全管理体系 要求(Information technology—Security techniques—Information security management systems—Requirements)

3 术语和定义

下列术语和定义适用于本文件。

3.1

公有云平台 cloud platform

一般为第三方服务商为客户提供的能够使用的资源。

3.2

堡垒机 fortress machine

在特定的网络环境下，为保障网络和数据不受来自外部和内部用户的入侵和破坏，而运用各种技术手段实时收集和监控网络环境中每一个组成部分的系统状态、安全事件、网络活动的机器，以便集中报警、及时处理及审计定责。

4 缩略语

下列缩略语适用于本文件。

DDoS:分布式拒绝服务攻击(Distributed Denial of Service)

SOP:标准操作程序(Standard Operating Procedure)

SLA：网络服务供应商和客户间的服务协议（Service-Level Agreement）
SSH：建立在应用层基础上的安全协议（Secure Shell）

5 基本要求

5.1 云服务商认证资质

云服务商应具备信息服务、数据安全等相关认证资质，如云计算等级保护四级测评、Service Organization Control（SOC）审计、CSA STAR 云安全国际认证金牌、PCI DSS 支付卡行业数据安全标准认证、ISO/IEC 27001：2013、ISO/IEC 20000-1：2011、ISO/IEC 20000-2：2012、ISO/IEC 22301：2012 等。

5.2 云服务商能力要求

5.2.1 底层技术能力

云平台软件漏洞或出现安全漏洞时，云服务商能够第一时间进行修复，保证底层云平台自身的安全，确保云租户之间的资源隔离。

5.2.2 云计算资源

拥有充足的云计算资源（包括数据中心、网络带宽、服务器等），满足云租户的应用需求，确保服务的可持续性。

拥有能够满足系统需要的库存管理能力和集群管理能力，降低运营成本，提高服务质量。

5.2.3 监控和应急处置能力

能够迅速发现或预测故障，同时拥有满足业务需求的故障迁移能力，确保在故障发生后能够迅速恢复服务。

5.2.4 风险管理能力

建立完善的风险管理体系，保证云平台自身的业务连续性。

5.2.5 内控合规体系

拥有健全的内控合规体系，采取资源隔离、访问控制、多副本存储、数据加密、运维审计等管理手段和技术措施，确保云租户数据不被未授权访问和使用、不发生内部数据泄露等事件。

5.2.6 安全服务增值能力

具备提供增值安全服务的能力，为云租户提供防 DDoS 攻击、防漏洞注入、防入侵等安全防护手段，帮助云租户免受网络攻击威胁。

5.2.7 安全审计能力

具备在网络边界、重要网络环节节点进行安全审计、对用户的重要行为和重要安全事件进行审计的能力。

5.2.8 SLA 标准

云服务商提供的资源应满足 SLA 协议标准。

5.3 运维人员要求

运维人员应满足以下要求：

a) 熟悉云资源申请、扩容、释放流程；
b) 熟悉公司 SOP 标准操作流程；
c) 了解公司使用的主流的操作系统和中间件；
d) 经过系统化的安全培训；
e) 从事 Linux 或 Window Server 运维工作不少于一年。

6 安全管理

6.1 网络安全

网络安全应满足以下要求：

a) 云平台系统对公网发布均应先安全检测并进行相关端口扫描后；
b) 云平台系统主机的运维工作宜从专线通过堡垒机进行；
c) 云主机宜通过负载均衡与互联网进行交互；
d) 云平台系统连接数据库宜通过专线或内部地址进行连接，禁止任何方式在互联网发布数据库端口；
e) 公司内网与云网络的互联互通需通过不同运营商的 2 条专线或 VPN 线路实现，互为备份，其中 1 条线路供公司内部系统与云平台系统对接使用，另 1 条线路供运维人员进行日常运维工作使用；
f) 云平台系统主机应在网络边界或区域之间根据访问控制策略进行访问规则设置。

6.2 资源安全

主机安全应满足以下要求：

a) 主机操作应该满足公司现行的各类操作系统安全配置规范及基线要求；
b) 主机部署中间件的版本和安全配置应该符合公司现有安全配置规范及基线要求；
c) 定时进行安全漏洞、安全基线扫描；
d) 为每个运维人员提供独立的运维账号，避免账号共享；
e) 对外提供服务前应提交申请进行安全漏洞检测，确定无高风险漏洞后，方可使用；
f) 应该部署主机防护、防病毒等主机安全类产品；
g) 主机默认情况下除允许通信端口，其他端口拒绝所有通信，应根据回话状态信息为进出数据流提供明确的允许/拒绝访问的能力。控制力度为端口级。

6.3 权限安全

6.3.1 业务维度权限管理

针对不同的业务系统，分配不同的账号，每个账户只对账户内的资源拥有管理权限。

6.3.2 资源维度权限管理

针对不同的资源，分配不同的账号，每个账户只对账户内的资源拥有管理权限。

6.4 环境安全

6.4.1 软件环境

云平台使用的操作系统和中间件,宜使用云服务商提供的模板或者开源系统。使用涉及版权的系统或中间件,应提前购买授权。需定期更新,打补丁保持软件的持续更新。

6.4.2 硬件环境

硬件环境宜使用云服务商提供的环境,硬件环境宜在国内部署。

示例:由服务商提供 mysql 数据库。

6.5 应用安全

应用安全应满足以下要求:

a) 基于 http/https 协议的应用发布,宜购买 web 应用防火墙等防护服务;
b) 对公网发布的应用系统宜通过负载均衡进行发布;
c) 云平台系统每年至少进行 2 次安全漏洞扫描检测;
d) 云平台系统不宜使用明文密码进行数据库连接;
e) 云平台应用发布流程标准不低于内部发布标准;
f) 所有变更操作要有变更记录,归档保存;
g) 云平台应用如涉及敏感数据宜进行加密处理。

7 资源管理

7.1 主机类资源管理

7.1.1 账号管理

系统管理员根据业务性质分配不同的账号并配置相应权限。

7.1.2 权限管理

系统管理员根据流程要求审核并授予权限。并记录。

7.1.3 容量管理

系统管理员根据资源配置需求扩展系统资源,负责分区及空间扩展工作,以及共享存储的挂载等工作。

7.1.4 日常管理

系统管理员进行操作系统的日常配置及变更操作,包括新建系统用户、口令管理、FTP、NTP、权限变更、安全配置变更及其他系统配置变更操作等。

7.1.5 故障管理

系统管理员跟进主机级的故障分析;会同开发、网络、系统、安全等团队处理系统故障并出具故障分析报告。

7.1.6 安全管理

系统管理员配合安全部门配置主机出入口安全。

7.1.7 备份管理

系统管理员根据对非结构化文件备份的情况对备份策略进行优化，包括备份时间、备份类型、保留时间等，在发生误操作或其他错误等需要恢复数据时进行恢复操作。

7.1.8 监控管理

系统管理员对业务系统进行操作系统级的监控配置和管理，包括系统容量、性能、可用性监控。及时处理系统故障，提供容量、性能分析报告。

7.1.9 趋势管理

系统管理员保持对业界新产品的跟踪，不断推动主机体系的优化。

7.2 数据类资源管理

7.2.1 账号管理

系统管理员根据业务性质分配不同的账号并配置相应权限。

7.2.2 权限管理

系统管理员根据流程授予权限并记录。

7.2.3 容量管理

系统管理员根据资源配置需求扩展系统资源空间。

7.2.4 日常管理

系统管理员除了对数据查询外，日常发版、数据变更、结构变更等操作，宜由需求方提供流程与脚本，然后系统管理员审核并执行脚本。

7.2.5 故障管理

系统管理员跟进数据级的故障分析；会同开发、网络、系统、安全等团队处理系统故障并出具故障分析报告。

7.2.6 安全管理

系统管理员配合安全部门配置数据出入口安全，审计对服务器和数据的操作行为。

7.2.7 备份管理

系统管理员根据流程描述在云平台部署数据备份策略。

7.2.8 监控管理

系统管理员根据监控要求对数据配置监控策略。

7.2.9 趋势管理

系统管理员保持对业界新产品的跟踪，不断推动数据体系的优化。

7.3 中间件类管理

7.3.1 账号管理

系统管理员根据业务性质分配不同的账号并配置相应权限。

7.3.2 权限管理

系统管理员根据流程授予权限，并记录。

7.3.3 容量管理

系统管理员分析用户量与资源之间比例关系。上线前审核压力测试过程与结果，根据资源配置需求评估连接数据库连接大小配置，对中间件进行相应的优化和提出扩容建议。

7.3.4 日常管理

系统管理员进行日常配置操作，包括中间件用户权限、口令、端口配置等各种中间件配置。

7.3.5 故障管理

系统管理员对业务系统跟进中间件级的故障分析；会同开发、网络、系统、安全等团队处理系统故障并出具故障分析报告。

7.3.6 安全管理

系统管理员配合安全部门配置中间件出入口安全，防范 DOS 等流量攻击。

7.3.7 备份管理

系统管理员备份中间件配置，保留到数据中心。

7.3.8 监控管理

系统管理员根据监控要求对中间件配置监控策略。

7.3.9 趋势管理

系统管理员保持对业界新架构新产品的跟踪，不断推动中间件部署体系的优化。

7.4 网络类资源管理

7.4.1 信息管理

网络管理员根据云平台业务使用需求，详细沟通确认双方互联方式，包括互联 IP 地址使用、双方业务系统 IP 地址、拟采用的网络互联技术、路由指向、策略管控等信息。

7.4.2 日常管理

网络管理员根据沟通确认结果，协调双方联调时间窗口，并实施联调，包括双方线路联通性联调、双方服务器间互通联调等。

7.4.3 权限管理

网络管理员根据业务系统间互访需求，进行互访权限设定及实施。根据业务部门提出的变更需求，在流程审批通过后完成路由、权限等信息的变更操作。

7.4.4 监控管理

网络管理员对与云平台互联线路的连通性进行监控配置和管理，及时处理线路故障问题。

7.5 安全类管理

7.5.1 漏洞管理

云业务系统部署完成后，安全运维人员及时对业务系统进行上线安全漏洞扫描，对扫描结果进行评估分析，协助系统相关人员完成漏洞整改工作，直到扫描无高风险漏洞，方可上线。

7.5.2 扫描管理

安全运维人员对云平台业务系统进行定期安全扫描工作，及时对业务系统进行上线安全漏洞扫描，对扫描结果进行评估分析，协助系统相关人员完成漏洞整改工作，确保系统的安全稳定。

7.5.3 防护管理

安全运维人员对云平台应用系统添加云安全防护，并监控云安全防护相关安全事件，及时对恶意攻击行为进行应急处理。

7.5.4 趋势管理

安全运维人员保持对业界安全事件的关注，及时优化安全体系。

7.6 监控类资源管理

7.6.1 权限管理

系统管理员根据流程授予权限并记录。

7.6.2 日常管理

系统管理员每日定时检查监控系统是否正常，是否存在需要调整的监控指标，协助添加、修改、删除监控信息，做好登记工作。

7.6.3 报警管理

对于监控报警事件，系统管理员及时反馈并联系相关人员进行处理。做好处理记录。

8 数据管理

8.1 数据迁移

一般数据进行敏感字段筛查后再进行数据迁移，可以利用云服务商提供的工具直接进行转换并者迁移。也可以通过服务商的合作伙伴进行迁移策略的制定和实施，其中：

a） 重要数据应对敏感字段进行脱敏或者加密后在进行数据迁移，保证数据安全；

b） 核心数据应根据公司的战略规划确定是否全部上云，上云数据敏感字段要做好加密和备份。

8.2 数据加密

在数据加密时应考虑如下情况：

a） 云平台数据加密应符合数据加密相关标准的要求；

b） 云平台与其他应用程序和数据一同工作的过程，如果需要操作明文数据，宜进行加密处理；

c） 云平台存储的数据涉及敏感字段，宜进行加密处理；

d） 数据在传输过程中应处于加密状态。

8.3 数据备份和回传

云平台上的数据建议进行如下操作：

a） 定期对云平台重要数据按照数据安全要求进行备份并校验数据正确性；

b） 核心数据备份副本宜同时备份到本地服务器一份；

c） 迁云数据在迁移前宜和云服务商协定数据回迁方案。

9 应急管理与培训

9.1 安全应急管理

每天对云资源监控主要指标进行巡检，重点对网络流出流量、CPU 使用率、内存使用率、存储空间变化、数据库压力等关键指标进行主动检查，对异常指标跟踪观察并通知使用人进行分析，对设置不合理的指标要及时调整。及时查看云平台发布的平台维护通知，评估影响并及时通知云租户。

出现紧急事件时，按照企业自有 SOP 操作程序执行。

9.2 故障应急管理

在云平台资源和系统出现报警时，根据下列情况进行分类处理：

a） 收到应用级报警信息时，根据报警内容联系各系统运维人员进行处理；

b） 收到系统级报警信息时，根据报警内容联系主机运维人员进行处理；

c） 收到平台级报警信息时，及时联系云服务商确认故障规模、影响范围、恢复时间、应急方案，及时向领导汇报情况并进行相应处理；

d） 出现其他紧急事件时，按照企业自有 SOP 操作程序执行。

9.3 培训

定期针对系统管理员进行培训，培训内容可包括下述内容：

a） 定期联系云服务商对云产品的迭代、新增进行讲解；

b） 定期对运维人员进行安全培训；

c） 定期对运维人员进行云运维技术考核和专项演练。