华为云中华人民共和国香港特别行政区保险行业监管遵从性指南

文档版本 1.1

发布日期 2022-05-16

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 概述

1.1 背景与发布目的

信息科技的迅速发展，为中华人民共和国香港特别行政区（下文简称“中国香港”）金融机构带来了显著的效益，但同时也为金融机构创造了一个复杂的环境。中国香港保险业监管局（The Insurance Authority，简称IA）是一个独立于政府的保险监管机构，其宗旨是维持保险业的稳定发展，并符合国际保险监管要求。为了规范保险行业对于信息科技的运用，保监局发布了一系列监管要求和指南，针对获准从事保险业务的机构或组织（获授权保险人，Authorized Insurer，简称AI）在网络安全、信息科技外包、网络保险活动管理等方面提出了相关监管要求。

华为云作为云服务供应商，致力于协助AI客户满足这些监管要求，持续为AI客户提供遵从保险行业标准要求的云服务及业务运行环境。本文将针对中国香港AI在使用云服务时通常需遵循的监管要求和指南，详细阐述华为云将如何协助其满足监管要求。

1.2 适用的中国香港保险行业监管要求简介

- **网络安全指引（Guideline on Cybersecurity，GL20）**：该政策文件旨在订明获授权保险人在网络安全方面应达到的最低标准，以及保监局在评价保险人的网络安全框架的成效时所采用的一般指导原则。
- **外判指引（Guideline on Outsourcing，GL14）**：该政策文件列出保监局期望获授权保险人在制订和监察外判安排时应考虑的重要事项，以保障现有和准保单持有人的利益。本指引亦阐述保监局用以监察获授权保险人的外判安排的方式。
- **网上保险活动指引（Guideline on the Use of Internet for Insurance Activities，GL8）**：该政策文件概述了获授权保险人在从事基于网络保险活动时需要注意的事项。

1.3 名词定义

- **华为云**

  华为云是华为的云服务品牌，致力于提供稳定可靠、安全可信、可持续创新的云服务。
- **保监局**

指中国香港保险业监管局（The Insurance Authority，简称IA）。

- **服务提供者/服务提供商**

  包括位于中国香港或中国香港以外地方的服务提供者，而该服务提供者可以是独立的第三者、与获授权保险人有关的一方（例如该保险人的附属公司或同一集团的附属公司）或隶属该保险人的单位（例如总办事处或海外分公司）。

- **外判/外包**

  指一项安排，而根据该安排，服务提供者承诺提供原本由获授权保险人本身提供的服务（包括业务活动、职能或程序）。

- **海外外判/海外外包**

  指一项关乎获授权保险人在香港营运的外判安排，而有关服务是在香港以外的地方提供，不论服务提供者在何处注册成立。

- **重要外判/重要外包**

  指一项外判安排，如根据该安排提供的服务中断或未达到可接受的标准，获授权保险人的财政状况、业务运作、信誉，或其对保单持有人履行责任或提供足够服务或其遵从法律及监管要求的能力，便可能大受影响。

- **客户内容数据**

  客户使用华为云服务过程中存储或处理的内容，包括但不限于数据、文件、软件、图像、音频、视频等类型的数据。

2 华为云的认证情况

华为云继承了华为公司完备的管理体系以及IT系统的建设和运营经验，对华为云各项服务的集成、运营及维护进行主动管理，并持续改进。截至目前，华为云已获得众多国际和行业安全合规资质认证，全力保障客户部署业务的安全，主要包括：

全球性标准类认证

认证	描述
ISO 20000-1:2011	ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的IT服务来满足客户和业务的需求。
ISO 27001:2013	ISO 27001是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。
ISO 27017:2015	ISO 27017是针对云计算信息安全的国际认证。ISO 27017的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO 22301:2012	ISO 22301是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
SOC审计	SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。
PCI DSS认证	支付卡行业数据安全标准（PCI DSS）是由JCB、美国运通、Discover、万事达和Visa等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。

认证	描述
CSA STAR金牌认证	CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
国际通用准则CC EAL3+	CC(Common Criteria)认证是一种信息技术产品和系统安全性的评估标准，它提供了一组通用的安全功能要求和安全保证要求，并在这些保证要求的基础上提供衡量IT安全性的尺度（即评估保证级EAL），使得独立的安全评估结果可以互相比较。
ISO 27018:2014	ISO 27018是专注于云中个人数据保护的国际行为准则。ISO 27018的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。
ISO 29151:2017	ISO 29151是国际个人身份信息保护实践指南。ISO 29151的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。
ISO 27701:2019	ISO 27701规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过ISO27701表明了其在个人数据保护具有健全的体制。
BS 10012:2017	BS 10012是BSI发布的个人信息数据管理体系标准，BS10012认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。
M&O认证	Uptime Institute是目前全球公认的数据中心标准化组织和权威的专业认证机构。华为云数据中心已获得Uptime Institute颁发的全球顶级数据中心基础设施运维认证(M&O认证)。获得M&O认证象征着华为云数据中心运维管理已处于国际领先水平。
NIST网络安全框架(CSF)	NIST CSF由标准、指南和管理网络安全相关风险的最佳实践三部分组成，其核心内容可以概括为经典的IPDRR能力模型，即风险识别能力（Identify）、安全防御能力（Protect）、安全检测能力（Detect）、安全响应能力（Response）和安全恢复能力（Recovery）五大能力。
PCI 3DS认证	PCI 3DS标准，旨在保护执行特定3DS功能或者存储3DS数据的3DS环境，支持3DS的实施。PCI 3DS的评估对象为3D协议执行环境，包括访问控制服务器、目录服务器或3DS服务器功能；以及3D执行环境内和连接到环境所需要的系统组件，如防火墙、虚拟服务器、网络设备、应用等；除此之外，还会评估3D协议执行环境的过程、流程、人员管理等。

地区性标准类认证

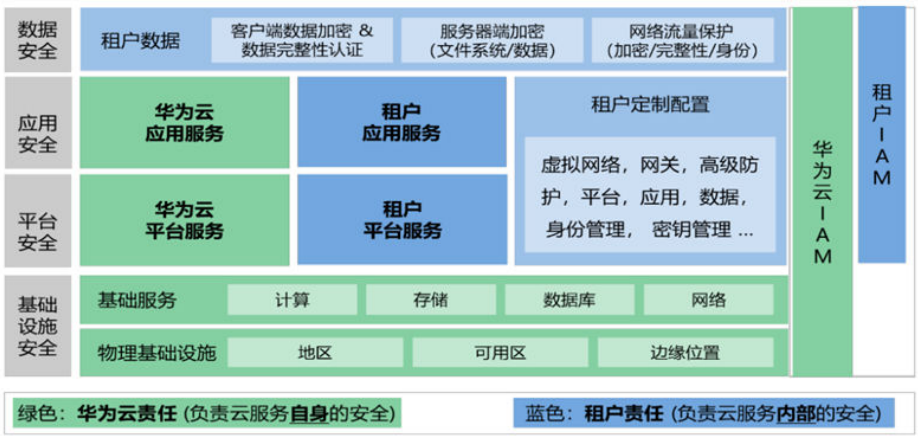
认证	描述
网络安全等级保护	网络安全等级保护是中国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键Region、节点通过了网络安全等级保护四级。
新加坡 MTCS Level 3 认证	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level 3等级认证。
可信云金牌运维专项评估	金牌运维评估是面向已通过可信云服务认证的云服务供应商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、健全的运维管理体系，符合国内权威云服务运营和维护保障要求的认证标准。
云服务用户数据保护能力认证	云服务用户数据保护能力评估是针对云服务用户数据安全的评估机制，评测关键指标范围包括事前防范、事中保护、事后追溯三个层面。
工信部云计算服务能力 评估	云计算服务能力评估是以《信息技术云计算云服务运营通用要求》等相关国家标准为依据的分级评估标准。华为私有云和公有云双双获得云计算服务能力“一级”符合性证书。
可信云评估	可信云评估是由数据中心联盟（DCA）组织、中国信息通信研究院（工信部电信研究院）测评的面向云计算服务和产品的权威评估。
网信办网络安全审查	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。

关于更多华为云的安全合规信息以及获取相关合规证书，可参见华为云官网“**信任中心-合规中心**”。

3 华为云安全责任共担模型

在复杂的云服务业务模式中，云安全不再是某一方单一的责任，需要租户与华为云共同努力。基于此，华为云为帮助租户理解双方的安全责任边界、避免出现安全责任真空区而提出了责任共担模型。在模型中租户与华为云具体负责的区域可参见下图。

图 3-1 责任共担模型



基于责任共担模型，华为云与租户主要承担如下责任：

华为云：主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和用户身份管理（IAM）层的多维立体安全防护体系，并保障其运维运营安全。

租户：主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和 IAM 层的各项安全防护措施的定制配置、运维运营安全、以及用户身份的有效管理。

关于华为云与租户的安全责任详情，可参考华为云已发布的**《华为云安全白皮书》**。

4 华为云全球基础设施

华为云目前已陆续在全球多个国家或地区开服。华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。关于更多关于华为云基础设施的信息，参见华为云官网“**全球基础设施**”。

5 华为云如何遵从及协助客户满足 IA《网络安全指引》的要求

中国香港保险监管局会于2019年6月发布了《网络安全指引》（2020年1月1日生效）。该规定从网络安全策略与框架、识别评估及控制风险、持续监控、响应与恢复、信息共享与培训等领域提出对获授权保险人网络安全管理的相关要求。

获授权保险人在遵循《网络安全指引》要求时，华为云作为云服务供应商，可能会参与到该要求所涉及的部分活动中。以下内容将总结《网络安全指引》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助获授权保险人满足这些控制要求。

5.1 网络安全策略与框架

原文编号	控制域	具体控制要求	华为云的应答
4.1-4.4	网络安全策略与框架	4.1获授权保险人应制订和维持网络安全策略与框架，而该策略与框架应以纾减与其业务性质、规模和复杂程度相的相关网络风险而建构。该网络安全策略与框架应经由该保险人的董事局审批。 4.2保险人在制订网络安全策略与框架时，应考虑其业务性质、规模、复杂程度和风险状况，并可参考或以科技及现有最佳并切实可行的质量保证标准作基准。 4.3网络安全框架应清楚界定该保险人的网络安全目标及对相关人员或系统使用者的能力要求。该网络安全框架应包含清晰明确的流程及所需的技术，以管理网络风险及适时将网络安全策略传达予所有使用者。 4.4保险人应定期检讨并更新其网络安全策略，以确保该策略在其业务经营模式和外在营商环境（包括外部网络风险情况）发生重大转变时仍然适用。	客户应基于其业务性质、规模、复杂程度和风险状况来制定网络安全策略与框架，并定期进行复核和更新以确保其适用性。作为云服务提供商： **（1）**华为云参照ISO27001构建了完善的信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性。全方位保护客户系统和数据的保密性、完整性和可用性。 **（2）**华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。 **（3）**华为云已通过ISO27001、NIST CSF、ISO27017、ISO27018、SOC、CSA STAR等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。

5.2 识别评估及控制风险

原文编号	控制域	具体控制要求	华为云的应答
6.1-6.2	识别评估及控制风险	6.1保险人应识别网络风险，并评价纾减措施的成效，以便在董事局或其指定的管理团队所订定的风险偏好和容许限额的范围内，抵御并管理网络风险。 6.2保险人应定期检讨网络风险应对程序，并在组织与经营结构和系统有重大改动时评价该等程序有否必要作出变更。例如，保险人应每年进行一次检讨或于系统作出重大改动后进行检讨。	客户应制定网络风险管理机制，定期开展网络风险评估，复核风险应对程序。作为云服务提供商，华为云遵从华为公司的信息安全风险管理框架，对风险管理范围、风险管理组织以及风险管理过程中的标准进行了严格定义。华为云每年进行一次风险评估，并且在信息系统发生重大变更、公司业务发生重大变化或适用的法律法规、标准发生重大变化时，华为云会进行相应风险评估。

5.3 持续监控

原文编号	控制域	具体控制要求	华为云的应答
7.1、7.2、7.4	网络安全监控	7.1保险人应建立系统性监察程序，以便能及早侦测网络安全事件、定期评价内部管控程序的成效、以及在适当情况下更新其风险偏好和容许限额。 7.2保险人应制定有效的监察措施，当中包括网络监察、测试、内部审计和外部审计等。 7.4保险人应最少每年测试一次其网络安全框架的所有组成部分，以决定其整体成效。保险人可使用一个或多个最新的方法和实践，例如安全漏洞评价、情景为本的测试及渗透测试。	客户应建立网络安全监控机制，采取有效的监控措施，包括部署网络监控、渗透测试、内部和外部审计。此外，客户还应每年对其网络安全框架的有效性进行测试，测试方式可考虑安全漏洞评估、情景模拟演练、渗透测试等。为配合客户满足监管要求： **（1）**华为云的**云监控服务（CES）**为客户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。可协助用户快速获取对云资源的告警，并采取相应的应对措施。同时华为云还可提供**Anti-DDoS流量清洗服务**、**DDoS高防（AAD）**、**Web应用防火墙服务（WAF）**、**数据库安全服务（DBSS）**、**云审计服务（CTS）**可帮助用户精准有效地实现对流量型攻击和应用层、数据层攻击的全面防护，以及事后对安全事件进行追溯和审计的功能。 **（2）**针对公有云攻击的手段多样、流量巨大的特点，华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速识别已经发生的攻击，并预判尚未发生的威胁。 **（3）**华为云定期会开展内部网络安全实战演练（如红蓝对抗）和第三方渗透测试和安全评估，监控、排查并解决安全威胁，保障云服务的安全性。 **（4）**华为产品安全事件响应团队（PSIRT）已经建立成熟的漏洞响应机制，针对华为云的自运营的特点，通过持续优化安全漏洞的管理流程和技术手段，以保证基础设施、平台、应用和云服务中的自研和第三方漏洞尽快修复，降低对用户业务造成影响的风险。同时，华为PSIRT和华为云安全运维团队已经建立了漏洞感知、处置和对外披露的机制。华为云依托其建立的漏洞管理体系进行漏洞管理，使基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在SLA时间内完成响应

原文编号	控制域	具体控制要求	华为云的应答
			和修复，降低并最终避免漏洞被恶意利用而导致影响用户业务的风险。 （5）华为云目前已获得多项国际上权威的安全与合规认证。华为云每年会聘请专业的第三方审计机构对华为云提供的云计算产品和服务进行审计。
7.3	身份认证与违规操作监控	作为监察程序的一部分，保险人应管理在实地和远程存取信息资产时所需的身份和验证数据。保险人应识别潜在网络风险的信号，或监察在其系统中是否已发生确实违规情况。	客户对访问信息资料的身份和凭证进行管理，通过实施监控措施，识别潜在风险，以及审查违规行为。为配合客户满足监管要求： （1）客户可通过华为云的**统一身份认证服务（IAM）**对使用云资源的用户账号进行管理。每一位华为云客户在华为云都拥有唯一可辨识的用户ID，并提供多种用户身份验证机制，包括账号密码、多因素认证等。 （2）华为云的**云审计服务（CTS）**可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 （3）华为云内部建立了运维和运营账号管理机制。华为云运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。此外，还采用双因子认证对华为云运维人员进行身份认证，如USB key、Smart Card等。所有运维账号由LDAP集中管理，通过统一运维审计平台集中监控并进行自动审计,以实现从创建用户、授权、鉴权到权限回收的全流程管理,并根据不同业务维度和相同业务不同职责，实行RBAC权限管理，保证不同岗位不同职责人员限定只能访问本角色所管辖的设备。

5.4 响应与恢复

原文编号	控制域	具体控制要求	华为云的应答
8.1-8.5	响应与恢复	8.1保险人应制订一个网络安全事件应变方案，涵盖网络安全事件的各种情景和相应的应变策略，以便在该等情景中维持并恢复各项关键功能和必要活动。应变方案亦应包括须向董事局或其指定的管理团队上报该等应变和恢复活动的准则。 8.2如发生网络安全事件，保险人应评估该事件的性质、范围和影响，并采取所有即时切实可行的措施，以控制该事件并纾减其影响。 8.3保险人应通知内部利益相关者和外部利益相关者（如适用），并在有需要时考虑采取联合应变行动。为此，保险人应最少每年进行一次事件应变演习。 8.4在侦测到相关事件后，保险人应在切实可行范围内尽快向保监局汇报该事件和相关数据，不管在任何情况下，该保险人须在侦测到该事件后的72小时之内向保监局汇报。 8.5在业务运作恢复稳定后，保险人应在相关事件的恢复过程中，识别并纾减所有被利用的安全漏洞，并就该安全漏洞加以纠正以避免同类事件再发生。	客户应建立安全事件管理机制，制定涵盖各类安全事件的应对策略，应包括事件处置、事件通知、事件上报、事件复盘等方面，另外客户还应定期开展安全事件应急演练。作为云服务提供商： **（1）**如果需要华为云协助执行客户的应急演练，华为会积极配合。 **（2）**华为云内部制定了完善的安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有7*24的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云使用大数据安全分析系统，关联各种安全设备的告警日志进行统一分析。根据安全事件对客户业务的影响程度进行事件定级，并启动客户通知流程，将事件通知客户。通知内容包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。 **（3）**基于云面临环境下存在复杂的安全风险，华为云制定了各类的专项应急预案，每年会对重大的安全风险场景进行应急演练，从而在发生此类安全事件时，快速削减可能产生的安全风险，保障网络韧性。 **（4）**华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。

5.5 信息共享与培训

原文编号	控制域	具体控制要求	华为云的应答
9.2	信息共享与培训	保险人应因应其面对的网络风险的类别和程度，就网络安全意识和网络安全的最新发展，安排所有系统使用者接受充分培训。保险人宜提升其员工（尤其是负责网络安全和系统的员工）的专业胜任能力。	客户应建立网络安全培训机制，定期对内部员工进行网络安全发展和网络安全意识的培训。作为云服务提供商，为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，华为对全体员工从意识教育普及、宣传活动开展、员工商业行为准则（BCG）承诺书签署三个方面开展安全意识教育。参考业界优秀实践，华为建立了完备的网络安全培训体系。在员工入职、在岗、晋升等环节纳入多种形式的安全技能培训，提升员工安全技能，提升员工能力，向客户交付安全的产品、解决方案与服务。为了内部有序管理，消减人员管理风险对业务连续性和安全性带来的潜在影响，华为云对运维工程师等重点岗位实施专项管理，包括：上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。更多关于内容请参见**《华为云安全白皮书》**4.4人力资源管理。

6 华为云如何遵从及协助客户满足 IA《外判指引》的要求

中国香港保险监管局会于2017年6月发布了《外判指引》（2017年6月26日生效）。该规定从法律及监管责任、外判政策、重要性评估、服务提供者、风险评估、外判协议、资料保密、监察及管控、应变计划、海外外判安排、分判等领域提出对获授权保险人在信息科技外包管理的相关要求。

获授权保险人在遵循《外判指引》要求时，华为云作为云服务供应商，可能会参与到该要求所涉及的部分活动中。以下内容将总结《外判指引》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助获授权保险人满足这些控制要求。

6.1 法律及监管责任

原文编号	控制域	具体控制要求	华为云的应答
4.1、4.2	法律及监管责任	4.1虽然获授权保险人可因事制宜，以最有利于实现公司目标的方法营运，但其董事局和管理层对所有外判服务负有最终责任。该保险人的法律责任不会因服务外判而受到限制或局限。 4.2外判安排不会减轻获授权保险人遵从有关法例、规例和规则的责任。获授权保险人须遵从该条例及保监局所公布的指引。具体来说，获授权保险人必须确保备存妥善的账簿和纪录，在保监局提出要求时供其在香港查阅，而该保险人或服务提供者可迅速提供充足和最新的数据，以供检索。该保险人不应订立任何会妨碍保监局执行其法定职责的外判安排。	客户应遵从该条例及保监局所公布的指引，妥善保存相关记录并能够迅速提供给保监局进行查阅，客户的董事会和管理层对所有外包服务负有最终责任。作为云服务提供商，华为云提供了线上的**《华为云用户协议》**以及**《华为云服务等级协议》**，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。客户以及其监管机构对华为云的审计和监督权益，会根据实际情况在与客户签订的协议中进行约定。

6.2 外判政策

原文编号	控制域	具体控制要求	华为云的应答
5.1、5.2	外判政策	5.1在把服务外判之前，获授权保险人应制订外判政策，由董事局审批。外判政策应包括以下各项：（a）把服务外判的目的及审批外判安排的准则；（b）评价外判安排重要性的构架；（c）全面评价外判安排所涉风险的构架；（d）监察和管控外判安排的构架；（e）参与审批、评价和监察外判安排人士的身份、职能和职责，以及该等职责可如何授权和权限详情；以及（f）检讨机制，以确保外判政策及监察和管控程序足以配合该保险人不时转变的营运情况，并切合市场、法律及规管的发展。 5.2该保险人应把外判政策妥为记录在案，并确保设有程序，让所有有关人员都对政策清楚知悉和遵循。	客户应制定书面的外包政策，经过董事会的批准。外包政策应包括：外包的目的和批准外包的标准、评估外包安排重要性的框架、外包风险评估框架、监督和管理外包安排的框架、外包管理组织和职责等。作为云服务提供商，华为云制定了自身的供应商管理机制，从供应商的产品和供应商本身的内部管理都提出了安全需求。此外，华为云会对供应商进行定期的稽核，在服务过程也中会持续监控其服务质量并对供应商进行绩效评分，对安全绩效差的供应商进行合作降级处理。

6.3 重要性评估

原文编号	控制域	具体控制要求	华为云的应答
5.4	重要性评估	获授权保险人应制定用以评价外判安排重要性的框架。评价某项安排是否重要，可能涉及定性判断，并且视乎有关保险人的情况而定。考虑因素包括（但不限于）： （a）如外判服务中断或未达可接受的标准，对该保险人的财政状况（例如偿付能力和资金流动性）、业务运作（例如为客户提供足够的服务）和信誉有何影响； （b）如外判服务中断或未达可接受的标准，对该保险人能否维持足够的内部管控和遵从法律及规管规定有何影响； （c）外判开支占该保险人总营运成本的比例；以及 （d）另寻服务提供者，或自行提供外判的服务（如有需要）的难度和所需时间。	客户应制定用以评价外包安排重要性的框架，考虑的因素包括： （1）如果外包服务中断或未达可接受的标准，对该授权保险人客户的财政状况、业务运营和信誉造成的影响； （2）如果外包服务中断或未达可接受的标准，对该授权保险人客户维持适当内部控制和遵守适用的法律法规要求的能力造成的影响； （3）外包成本占该授权保险人客户总运营成本的比例； （4）寻找替代服务提供商或自行提供外包服务的难度和所需时间。

6.4 风险评估

原文编号	控制域	具体控制要求	华为云的应答
5.6	风险评估	在订立新的外判安排，或续订或修改现有的外判安排前，获授权保险人应全面评价拟议安排或修改所涉及的风险。进行评价时，应考虑所有相关风险，包括对财政、运作、法律和信誉的影响，以及一旦服务提供者未能提供外判服务，客户可能蒙受的损失。该保险人应尽职审查及谨慎评价，确保在实施拟议安排或修改前，已处理所识别的风险。	在订立新的外包安排，或续订或修改现有外包安排前，客户应对外包安排进行风险评估，考虑包括财务、运营、法律、声誉等方面的风险，并对外包服务提供商进行尽职调查。作为云服务提供商，为配合客户满足监管要求，华为云会安排专人积极配合客户的尽职调查，关于华为云在信誉、财务稳健度、风险管理能力、技术能力、运营能力、服务资质等方面的情况，请参见**本文档6.5服务提供者**下的**“尽职调查”**的相关内容。此外，华为云业务的开展遵循华为公司“一国一策，一客一策”的战略，在遵从客户所在国家或地区的安全法规以及行业监管要求的基础上，参考业界最佳实践从组织、流程、规范、技术、生态和等方面建立并管理完善、高可信、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放透明的方式，共同应对云安全挑战，助力客户的安全需求。

6.5 服务提供者

原文编号	控制域	具体控制要求	华为云的应答
5.8	尽职调查	获授权保险人在甄选服务提供者时，应尽职审查及谨慎评价，并考虑各项因素，如该服务提供者的总计风险承担、可能出现的利益冲突、从评价和甄选服务提供者而得的利益相对于外判的价格是否物有所值。此外，在评价服务提供者时，该保险人应考虑包括下列各项的因素： （a）服务提供者的信誉、经验和服务素质； （b）财政稳健程度，尤其是能否持续提供达到预期水平的服务； （c）管理技巧、技术和营运方面的专业知识和能力，尤其是能否处理服务中断的情况； （d）是否已取得法律规定的牌照、注册、许可或授权，以提供外判服务； （e）对分判商的依赖程度，以及监察分判商工作表现的成效； （f）能否配合该保险人的公司文化和未来发展策略；以及 （g）对保险业的熟悉程度，及能否紧贴市场的创新步伐，与时并进。	客户在选择服务提供商时，应对其进行尽职调查，涵盖信誉、财务稳健度、风险管理能力、技术能力、运营能力、服务资质等方面。作为云服务提供商，华为云在上述方面的情况如下： **（1）商业声誉**：华为云一如既往坚持“以客户为中心”，让越来越多的客户选择了华为云。在中国多个行业，例如互联网、点播直播、视频监控、基因、汽车制造等行业，华为云已实现突破。 **（2）财务稳健度**：华为云是华为的云服务品牌，自2017年正式上线以来,华为云一直处于快速发展中，收入保持强劲增长态势。全球权威咨询机构Gartner发布的《Market Share: IT Services, worldwide 2019》报告显示，华为云全球IaaS市场排名第六，中国市场排名前三，全球增速最快，高达222.2%。 **（3）风险管理能力**：华为云继承了华为公司的风险管理能力，建立了风险管理体系，并通过风险管理体系的持续运作，在复杂的内外部环境和巨大的不确定市场中有效控制风险，力求业绩增长和风险之间的最优平衡，持续管理内外部风险，保障公司持续健康发展。 **（4）技术能力**：华为云用在线提供云服务的方式，将华为30多年在ICT基础设施领域的技术积累和产品解决方案开放给客户。华为云具备全栈全场景AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在AI领域，华为云AI已在城市、制造、物流、互联网、医疗、园区等10大行业的300+个项目进行落地。在多元架构方面，华为云打造了基于X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，使客户价值最大化。 **（5）运营能力**：华为云遵循ISO27001、ISO20000、ISO22301等

原文编号	控制域	具体控制要求	华为云的应答
			国际标准建立信息安全管理体系、IT服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。 **（6）服务资质**：虽然中国香港对提供云服务没有特定的许可证或认证要求，但华为云有多种认证以保证其服务的安全和兼容操作，这包括ISO 27001、ISO 27017、ISO 27018、CSA STAR、PCI DSS等认证。更多认证信息请参见本文档**2.华为云的认证情况**。 **（7）适合金融机构的企业文化和服务政策：**华为云在产品和服务规划和阶段会根据客户业务场景、适用的法律法规及监管要求等方面对产品的安全和功能需求进行定义，并在研发设计阶段将功能实现，以满足客户的需求。华为云结合行业需求特点和华为丰富的云服务，发布了金融行业解决方案，为银行、保险等客户提供端到端的云解决方案。 **（8）对新发展作出反应的能力：**自上线以来，华为云一直坚持技术创新，发布了一系列业界领先的新品和升级，覆盖云安全、DevOps、云容器引擎和微服务引擎、服务网格、计算、云存储、网络、云容灾等多个领域，让产品始终保持先进性。 **（9）分包：**请参见本文档**6.11分判**的相关内容。

原文编号	控制域	具体控制要求	华为云的应答
5.9	定期复核	获授权保险人应定期（最少每年一次）检讨所标明服务提供者的能力（包括财力和技术能力），以评价服务提供者能否持续提供达到预期水平的服务。	客户应定期对服务提供商进行审查，以评估其服务能力。作为云服务提供商： **（1）**华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。 **（2）**华为云遵循ISO27001、ISO20000、ISO22301等国际标准建立信息安全管理体系、IT服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。

6.6 外判协议

原文编号	控制域	具体控制要求	华为云的应答
5.10	外判协议	外判安排应以具法律约束力的书面协议方式订立。获授权保险人与服务提供者商议合约时，应考虑包括以下各项的事宜：（a）外判服务的范围；（b）提供外判服务的地点；（c）外判安排的有效期；（d）该保险人及服务提供者的合约责任及法律责任；（e）外判服务提供者须达到的表现标准。如该保险人已向顾客保证履行某一服务标准或服务承诺，这点尤为适切；（f）该保险人欲向服务提供者要求提交报告或通知规定；（g）该保险人及服务提供者根据协议监察所提供服务的方式（例如透过服务报告评价表现、定期进行自我评核，以及由该保险人或服务提供者的核数师作出独立检讨）；（h）数据与资产的拥有权、信息技术保安及机密资料的保护；（i）有关分判的规则和限制，例如把外判的服务分判，须该保险人事先同意。如服务提供者使用分判商，该保险人应确保可继续对外判风险做出类似的管控；（j）针对服务提供者表现欠佳的补救行动及上报程序；（k）服务提供者有否制定应变计划，确保外判服务持续无间；（l）管理及审批有关修改外判安排的程序；（m）在什么情况下该保险人或服务提供者可终	客户应与服务提供商签订外包协议，并保证协议的合法性和适宜性。为配合客户行使对云服务供应商的监管，华为云线上的《对客户和华为的安全职责进行划分，华为云**《华为云服务等级协议》**规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的要求，在其中与客户共同约定相应要求。

原文编号	控制域	具体控制要求	华为云的应答
		止外判协议；（n）终止外判安排的协议，包括知识产权及数据的拥有权，以及订明有关程序，确保把外判服务顺利移交给另一个服务提供者或交回该保险人；（o）服务提供者做出的保证或弥偿，例如服务提供者保证，若把有关的外判服务分判，便会承担责任，包括分判商失责所引致的法律责任；（p）服务提供者须持有相关保险的规定；（q）因外判安排而可能引起的纠纷的调解机制；（r）服务提供者同意让该保险人的核数师和精算师及保监局取用任何簿册、纪录及数据，以便履行法定职责和责任；以及（s）管限外判协议的法律，最好是香港法律。	

6.7 资料保密

原文编号	控制域	具体控制要求	华为云的应答
5.12	数据的机密性	获授权保险人应确保外判安排符合有关客户资料保密的法例及法定要求（例如《个人资料（私隐）条例》（第486章））。该保险人也应确保本身和服务提供者都设有适当的保障措施，使本身及客户的数据完整和保密。	客户应采取适当的保障措施，确保外包服务符合客户资料保密的法律要求。为配合客户满足监管要求： **（1）**华为云不用客户数据做商业变现，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守适用的法律法规或政府机关的约束性命令，并严格遵守《个人资料（私隐）条例》（PDPO）所述的数据保护原则，更多信息请参见**《华为云中华人民共和国香港特别行政区PDPO遵从性说明》**。 **（2）**华为云各服务产品和组件从设计之初就规划并实现了合理的隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。

原文编号	控制域	具体控制要求	华为云的应答
5.13	客户通知与数据销毁	获授权保险人应履行法律或合约责任，把外判安排及客户资料可能外泄或遗失的情况通知客户。如果外判协议终止，该保险人便应确保取回服务提供者手中的所有客户资料或把数据销毁。	客户应建立通知机制，将外包安排和客户数据泄露事件向其客户通知。另外，应在外包协议终止后，回收或销毁保存在服务提供商手中的客户资料。为配合客户满足监管要求： （1）华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。 （2）当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循适用的法律法规，以及与客户之间的协议约定，按照数据销毁标准清除客户的数据。为了避免重要数据销毁后不可恢复，或因误操作丢失，建议客户在销毁数据之前慎重考虑，对拟销毁的数据做好备份或迁离。 ● **客户内容数据迁离：**华为云提供的**云数据迁移服务（CDM）**支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓库、文件等，并且支持在多个环境之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。 ● **客户内容数据销毁：**在客户内容数据的销毁阶段，华为云会对指定的数据及其所有副本进行清除。当客户确认删除操作后，华为云首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，使相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，使其上的数据无法恢复。

原文编号	控制域	具体控制要求	华为云的应答
5.14	对保监局报告事件	如服务提供者或其分判商擅自取用获授权保险人或其客户的数据或违反保密规定，以致对两者造成影响，该保险人应立即通知保监局。	当服务提供商泄露客户数据或违反保密规定时，客户应及时通知保监局。为配合客户满足事件上报保监局的要求，华为云设置7*24的专业安全事件响应团队以及专家资源池，依照适用的法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。

6.8 监察及管控

原文编号	控制域	具体控制要求	华为云的应答
5.15(c)(d)、5.16	监察及管控	5.15为了有效地监察和管控各项外判安排，获授权保险人应采取包括以下各项的措施： （c）应尽职审查及小心监察每项外判安排，以确保服务提供者以预期的方式提供服务，并适当履行外判协议所载的条文；以及 （d）定期（最少每年一次）进行检讨或稽核，以确保外判政策及监察和管控程序获得妥善遵行。 5.16获授权保险人实施外判安排后，应定期检讨其管控措施在监察服务提供者的表现和管理外判服务所涉风险方面是否有效和足够。该保险人应设立上报程序，让该保险人和服务提供者的管理层可迅速得知与外判服务有关的问题。如发现有欠妥之处，应立即采取适当的行动以纠正问题。如出现重大问题，致使该保险人的财政状况、业务运作或遵从法律及规管规定等方面可能大受影响，该保险人应当立即通知保监局。	客户应建立外包服务的监控机制，在外包服务开始前对服务提供商进行尽职调查，并定期对外包监控的政策和程序复核与审计，以便进行持续改善。作为云服务提供商： **（1）**华为云每年定期接受专业第三方审计机构的审计，并可在客户需要时可向其提供相关审计报告。华为云也会安排专人负责客户方发起的尽职调查。 **（2）**华为云作为云服务提供商，负责其提供的基础设施和IaaS、PaaS和SaaS各类各项云服务的事件和变更管理。华为云制定了事件和管理流程并定期对其评审和更新。华为云拥有7*24的专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的事件。并根据事件的实时状态进行事件升级和通报。且华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。 **（3）**华为云为客户提供售后服务保障，华为云专业的服务工程师团队提供7*24小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等寻求帮助，将问题升级。除基础支持以外，系统复杂的企业客户可以选择适用的支持计划，获取由IM企业群、技术服务经理（TAM）、服务经理等组成的专属支持。

6.9 应变计划

原文编号	控制域	具体控制要求	华为云的应答
5.17-5.18	应变计划	5.17获授权保险人若把服务外判，便应制订应变计划，以确保其业务不会因服务提供者突发的不良事故（例如系统故障）而中断。该保险人在制订应变计划时，应考虑和妥善处理以下事项： （a）是否已有后备设施或另一个服务提供者可提供服务，或可否把外判的服务改由该保险人自行提供； （b）如出现问题，导致业务不能持续运作，须予遵循的程序和负责有关行动的人员；以及 （c）定期检讨和测试应变计划的程序。 5.18获授权保险人也应确保服务提供者订有本身的应变计划，以应对日常运作和系统上的问题。该保险人应充分了解服务提供者的应变计划，并考虑若服务提供者出现突发的不良事故，导致外判服务受阻，对该保险人本身的应变计划有何影响。	客户应为外包给服务提供商的服务制定业务连续性计划，并定期对业务连续性计划进行审查和测试。另外，客户还应确保其服务提供商也制定了自身的业务连续性计划。为配合客户满足监管要求： **（1）**如果客户在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。 **（2）**华为云作为云服务供应商，为客户提供其业务所依赖的云服务，因此除不可抗因素导致的外包中断或意外终止的情况外，华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。 **（3）**客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

6.10 海外外判安排

原文编号	控制域	具体控制要求	华为云的应答
5.19	海外外判安排	获授权保险人在作出海外外判安排时，应特别留意以下各点： （a）国家风险—该保险人在作出海外外判安排时，应考虑所涉及的国家风险。这些风险包括有关海外司法管辖区的社会、经济和政治情况，以及其法律和规管制度。它们可能会令到服务提供者不能有效履行外判协议的条文，也不能有效监察外判服务和服务提供者的表现。 （b）数据保密—在某些情况下，海外主管机构（例如警方和税务机关）有权取用该保险人和客户的数据。该保险人应考虑有关机构有权取用数据的范围和可能性，并在其认为适当时，寻求法律意见，以求明确。如海外主管机构要求取用该保险人的客户资料，该保险人应立即通知保监局。 （c）通知客户—鉴于海外外判安排所带来的额外风险，该保险人应考虑是否有需要把提供有关服务所在的司法管辖区，以及海外主管机构所拥有取用数据的权利通知客户。	客户在进行海外外包安排时，应当考虑所涉及的国家风险、当地监管机构对其数据的访问权利、以及对客户的通知。作为云服务提供商： **（1）**华为云目前已陆续在多个国家和地区建立数据中心，相关位置可参见华为云官网“**全球基础设施**”。华为云在世界各地的数据中心都受到严格的保护，旨在保护客户数据免受伤害和未经授权的访问。华为云已实施环境控制，以保护数据中心，包括温度控制、供暖、通风和空调、火灾探测和灭火系统以及电源管理系统、24小时监控的物理硬件。 **（2）**华为云以区域为单位提供服务，区域也即是客户内容数据的存储位置，华为云未经授权绝不会跨区域移动客户的内容数据，除非（a）必须迁移以遵守适用的法律法规或者政府机关的约束性命令;（b）为了提供账单、管理、技术服务或者出于调查安全事件或调查违反合同规定的行为。客户在使用云服务时，依据就近接入原则、不同地域的适用的法律法规要求等进行区域的选择，使客户内容数据存储在目标位置。 **（3）**华为云业务的开展遵循华为公司“一国一策，一客一策”的战略，在遵从客户所在国家或地区的安全法规以及行业监管要求的基础上，参考业界最佳实践从组织、流程、规范、技术、生态和等方面建立并管理完善、高可信、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放透明的方式，共同应对云安全挑战，助力客户的安全需求。

6.11 分判

原文编号	控制域	具体控制要求	华为云的应答
5.20-5.21	分判	5.20如外判服务提供者获准把有关服务进一步外判，获授权保险人会因此而承担额外的风险。该保险人应设立足够的程序，以管控和监察这类分判安排，并确保服务提供者把有关服务进一步外判时，会考虑本指引所载的重要事项，犹如本身是有关的保险人一样。 5.21获授权保险人应在外判协议中加入有关分判的规则和限制，例如规定服务提供者须事先取得该保险人同意把有关服务分判，并须对分判商能否称职负上法律责任。该保险人应确保服务提供者的分判安排不会妨碍其履行与该保险人所订外判协议的条文，特别是有关资料保密、应变计划和监管机构数据取用权的规定。	客户应对服务提供商的分包安排进行监控，与服务提供商在外包协议中约定分包的规则和限制，确保分包安排不会影响服务提供商对外包协议的履行。为配合客户行使对科技外包的监管： （1）华为云线上的**《华为云用户协议》**对客户和华为云的安全职责进行划分，华为云**《华为云服务等级协议》**规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的要求，在其中规定华为云若聘用分包商，需通知客户，并对分包的服务负责。 （2）华为云制定了自身的供应商管理机制，从供应商的产品和供应商本身的内部管理都提出了安全需求。此外，华为云会对供应商进行定期的稽核。此外会与涉及网络安全的供应商签署网络安全协议，在服务过程也中会持续监控其服务质量并对供应商进行绩效评分，对安全绩效差的供应商进行合作降级处理。

6.12 监管方式 - 就重要外判安排作出事先通知

原文编号	控制域	具体控制要求	华为云的应答
6.1	监管方式 - 就重要外判安排作出事先通知	就重要外判安排而言，获授权保险人如计划订立新的安排或大幅修改现有安排，便应通知保监局。该保险人除非另有充分理据，否则应在拟订立新外判安排或大幅修改现有安排的日期最少三个月前作出通知。该保险人应令保监局信纳其已在计划阶段考虑并妥善处理本指引第5部所载的重要事项。保监局可在其认为适当的情况下，与该保险人讨论与外判安排有关的疑虑，并要求该保险人采取所需措施，以释除疑虑。如该保险人未能在三个月的事先通知期内释除疑虑以令保监局满意，保监局可把通知期延长。如三个月的事先通知期已届满，而保监局仍未就拟议外判安排或重大修改与该保险人沟通，则该保险人可视有关建议已为保监局所接纳，并可着手订立拟议安排或作出拟议修改。	当客户计划签订新的重大外包协议或对现有协议进行重大变更时，客户必须通知保监局。通知包括以下要求： **（1）**除非客户另有正当理由，否则通知应在拟订立新的外包安排或拟对现有安排作出重大改变之日前至少3个月发出。 **（2）**对拟签订的外包安排或现有外包安排的重大变更的详细说明。 **（3）**足够的信息，以使保监局满意，客户已经考虑并妥善解决了《外判指引》第5章中规定的所有重要事项。

7 华为云如何遵从及协助客户满足 IA《网上保险活动指引》的要求

中国香港保险监管局会于2017年6月发布了《网上保险活动指引》（2017年6月26日生效）。该规定从服务供应商的身份、授权情况、安全措施、通信方式等领域提出对获授权保险人在网络保险活动管理的相关要求。其中安全措施包括信息安全政策、数据完整性、数据机密性、备份管理等方面的要求。

获授权保险人在遵循《网上保险活动指引》要求时，华为云作为云服务供应商，可能会参与到该要求所涉及的部分活动中。以下内容将总结《网上保险活动指引》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助获授权保险人满足这些控制要求。

原文编号	控制域	具体控制要求	华为云的应答
5.1（a）	信息安全政策	订有全面及足以配合互联网保安科技发展的保安政策及措施；	请参见本文档**5.1网络安全策略与框架**的相关内容。

原文编号	控制域	具体控制要求	华为云的应答
5.1（b）	数据的完整性	制定适当的机制，以保持系统硬件所储存的数据、在传送中的数据以及在网站上显示的数据均完整无缺；	客户应采取适当措施确保数据在存储和传输过程中的完整性。为配合客户满足监管要求： **（1）**华为云数据存储采用多副本备份和纠删码设计，通过冗余和校验机制来判断数据的损坏并快速进行修复，即使一定数量的物理设备发生故障也不会影响业务的运行。例如**对象存储服务（OBS）**，通过以下2点保证数据的完整性和可靠性： • **数据检查：**存储前和存储后通过Hash校验数据一致性，使存入数据与是上传数据一致。 • **分片冗余：**数据分片后多份冗余存储在不同磁盘，后台自行检测一致性并及时修复受损数据。 **（2）**当客户通过互联网提供Web网站业务时，可以使用华为云联合全球知名证书服务商提供的证书管理服务。通过给Web网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输，保证数据的机密性和完整性。
5.1（c）	备份管理	有为数据库及应用软件而实施的适当备份程序；	客户应制定备份管理机制，对关键业务数据、数据库、应用软件进行适当的备份。作为云服务提供商，华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。客户可以使用**对象存储服务（OBS）**的版本控制、**云硬盘备份（VBS）**、**云服务器备份（CSBS）**等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云，保证在灾难发生时数据不丢失。
5.1（d）	数据的机密性	客户的个人资料（包括任何密码在内）备受保障，以免失去或未经授权被人取得、使用、修改或披露；	请参见本文档**6.7 资料保密**下**“数据的机密性”**的相关内容。

原文编号	控制域	具体控制要求	华为云的应答
5.1（f）	支付系统安全	电子付款系统（例如信用卡付款系统）安全稳妥；	客户采取适当措施确保支付系统的安全。目前，华为云作为云产品及服务的提供者，已经取得了基于3.2.1版本的PCI DSS一级认证，表明华为云的基础环境已经达到了PCI DSS的要求，可为客户提供高质量的数据安全保护。根据华为云安全责任共担模型，对于部署在华为云环境的部分，客户可以依赖华为云的符合性证明，但客户仍然需要满足PCI DSS的其他要求。更多信息请参见**《华为云PCI DSS实践指南》**。

8 结语

本文描述了华为云为客户提供的云服务如何遵从中国香港保险监管要求，并表明华为云遵守中国香港保险业监管局发布的重点监管要求，有助于客户详细了解华为云对于中国香港保险监管要求方面的遵从性，让客户安全、放心地通过华为云服务存储、处理客户内容数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署遵从中国香港保险行业监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

本白皮书仅供一般性参考，不具备任何法律效力或构成任何形式法律建议，客户应酌情评估自身使用云服务的情况，并负责确保在使用华为云时对相关中国香港保险行业监管要求的遵从性。

9 版本历史

日期	版本	描述
2022年4月	1.1	例行刷新
2020年9月	1.0	首次发布