亚马逊云科技 | pwc 普华永道

医药出海 直挂云帆

健康及生命科学行业出海合规实用指南

关于普华永道部分的声明：

本指南仅作为一般性指导，并不构成提供任何形式的法律咨询、会计服务、投资建议或专业咨询。本指南所提供的信息不能取代专业税收、会计、法律咨询或其他相关专业咨询建议。在作出任何决定或采取任何行动之前，您应该咨询专业顾问，并向其提供与您特定情况相关的所有事实。

本指南的信息来源于本次调研所收集的数据以及公开的资料，我们对信息的完整性、准确性或及时性概不作出任何保证或担保，也不提供任何明示或暗示的担保，包括但不限于对业绩、适销性和适用于特定用途的担保，在不同时期可能会得出与本指南不一致的观点。

本指南仅供一般参考使用，不构成具体事项和咨询意见，普华永道不对本指南内容承担审慎责任，并且未就本指南内容做出任何明示或暗示保证。普华永道不就本指南内容向任何人士承担任何责任或义务，也不向任何人士承担因本指南所引起的或与本指南有关的任何责任或义务。读者不应依赖本指南内容做出投资或其他商业决定。如需具体意见，请咨询专业顾问。

关于亚马逊云科技部分的声明：

本指南中由亚马逊云科技负责撰写的内容陈述了亚马逊云科技在封面页所示日期的有关服务产品及实践，该等信息可能变化且我们不会另行通知。读者对于本部分的信息以及亚马逊云科技的产品或服务应自己做出独立的判断，该等内容都是“依现状”提供，不包含任何明示或者暗示的保证。本部分内容并没有创设来自亚马逊云科技或其关联方、供应商或许可方的任何保证、陈述、合同性承诺、条件或者担保。亚马逊云科技对其客户的义务和责任均由适用的客户协议管辖。本部分内容不是亚马逊云科技和其客户之间任何协议的组成部分，也不构成对任何协议的修改。

引 言

近年来，国内医疗健康行业的投融资金额不断攀升，虽然由于疫情影响，自2022 年起投资热度略有降低，但医疗行业投资结构正面临转型，医药企业投资逐步呈现全球化布局的趋势，在跨境合作领域仍持续释放活力。同时，随着药品集采、医保谈判持续推进，国内医药企业发展空间被日益压缩，在此背景下，中国健康及生命科学行业的企业纷纷走出国门迈向海外市场，以寻找发展的沃土。

2022 年颁布的《“十四五”医药工业发展规划》也表达出寻求更深层次的国际化，加入到主流市场竞争的愿景。《规划》指出要创造国际竞争新优势。到 2025 年，主要经济指标实现中高速增长，前沿领域创新成果突出，产业链现代化水平明显提高，药械供应保障体系进一步健全，国际化全面向高端迈进。

在本文中，我们试图围绕健康及生命科学行业企业出海发展需要面对的相关数据安全法律法规、合规挑战，数字化解决方案和应对的最佳实践等方面展开探讨。

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

第一部分

海外关于数据保护相关的法律法规

自 21 世纪起，中国健康及生命科学行业企业开始探索国际化发展道路，从最初的化学原料药，到仿制药出海，继而创新药的全球布局，企业不断探索国际营运模式。同时，健康及生命科学行业企业面临全球创新及空前的互联性，应运而生的数据保护、数据合规已成为各国最重视合规要求之一，也是所有国际布局的健康及生命科学企业必须面对和解决的重要问题。本文列举了企业出海普遍选择的部分国家与地区关于数据方面的重要法律法规，具体见《表 1 ： 部分海外国家与地区关于数据方面的重要法律法规》。

表 1 ： 部分海外国家与地区关于数据方面的重要法律法规

国家	法规 / 标准名	生效年份	适用范围 / 领域
欧盟	《General Data Protection Regulation》* （中文：《通用数据保护条例》，简称“GDPR”）	2018 年	通用数据合规
欧盟	《Regulation on a framework for the free flow of non-personal data in the European Union》 （中文：《非个人数据在欧盟境内自由流动框架条例》，简称“FFDR”）	2018 年	非个人数据安全合规
美国	《Health Insurance Portability and Accountability Act》* （中文：《健康保险流通与责任法案》，简称“HIPAA”）	1996 年	个人健康信息的隐私和安全合规
美国	《Health Information Technology for Economic and Clinical Health Act”》* （中文：《经济与临床健康信息技术法案》，简称“HITECH”）	2009 年	经济与临床健康信息
美国	《Code of Federal Regulation :Title 21 Food and Drugs》* （中文：《美国联邦法规：第 21 篇 食品和药品》，简称 “21 CFR”）	1936 年	食品药品合规
美国	《Good Various Practice》《良好实践规范》，简称“GXP”	1936 年	药品生产管理
英国	《Data Protection Act 2018》 （中文：《2018 年数据保护法》）	2018 年	数据安全合规
英国	《UK General Data Protection Regulation》 （中文：《英国通用数据保护条例》，简称“UK GDPR”）	2021 年	通用数据合规
英国	《Privacy and Electronic Communications Regulations》 （中文：《隐私和电子通信条例》，简称“PECR”）	2003 年	隐私和电子通信合规
日本	《Pharmaceutical and Medical Device Act》 （中文：《日本药品和医疗器械法案 》，简称“PMD Act”）	2014 年	药品和医疗器械管理
日本	《Act on the Protection of Personal Information》 （中文：《个人信息保护法 》，简称“APPI”）	2003 年	个人信息保护
加拿大	《Canadian Medical Device Regulations》 （中文：《加拿大医疗器械法规》，简称“CMDR”）	2003 年	医疗器械
加拿大	《Canadian Food and Drug Regulations》 （中文：《加拿大食品药品条例 》，简称“C.R.C., c. 870”）	1985 年	药品管理
加拿大	《Personal Information Protection and Electronic Documents Act》 （中文：《个人信息保护及电子文档法案》，简称“PIPEDA”）	2001 年	个人信息保护
新加坡	《HEALTH PRODUCTS ACT 2007》 （中文：《卫生产品法 2007 》，简称“HPA2007”）	2007 年	药品管理
新加坡	《Personal Data Protection Act》 （中文：《2012 年个人数据保护法案》，简称“PDPA”）	2013 年	个人信息保护

备注：“*”法律法规将在第二章节进一步解读

第二部分

部分法律法规的进一步解读

欧洲和北美依然占据中国企业出海的首选目的地，下文针对欧盟国家严格执行的《通用数据保护条例》（简称“GDPR”）、美国应用范围较广且影响较大的《健康保险流通与责任法案》(简称“HIPAA”)、《经济与临床健康信息技术法案》(简称“HITECH”)和《良好实践规范》（简称“GxP”）进行进一步解读。此外，日本、加拿大和新加坡也是中国健康及生命企业出海选择的热门国家，下文对这些重要国家的数据安全管理相关的法律也进行了概述和解读。

2.1

欧盟国家严格执行的数据合规要求：《通用数据保护条例》（简称“GDPR”）

GDPR 概要

欧盟与 2018 年 5 月 25 日出台了 GDPR，对欧盟公民数据的处理制定了一套统一的法律和更严格的规定。GDPR 颁布框架如《图 1 GDPR 颁布框架》所示，条例概要如《图 2 GDPR 法规概要》所示。

图 1 GDPR 颁布框架

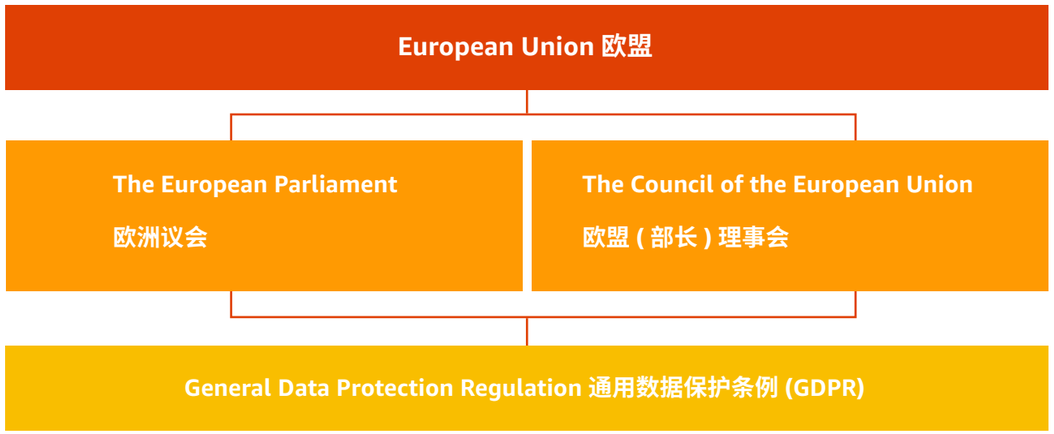


图 2 GDPR 法规概要

1 适用范围

欧盟境内有实体的企业；

欧盟境外企业：

- 面向位于欧盟的数据主体提供产品或服务
- 监控位于欧盟境内的数据主体发生在欧盟的行为

2 关键角色

数据主体

监管机构

数据控制者

- 确定个人数据外理的目的和方式

数据处理者

- 根据控制者指示处理个人数据

3 数据主体权利

- 知情权
- 访问权
- 更正权
- 拒绝权
- 删除权 (被遗忘权)
- 限制处理权
- 数据可携权
- 不受制于自动化决策

4 个人数据 & 特殊类别个人数据

已被识别

可被识别

种族或血统　**宗教或哲学信仰**

政治观点　**工会成员资格**

基因和生物信息

健康

性生活或性取向

5 对数据控制者和 / 或处理者的个人数据保护要求

安全保护　**数据处理记录**　**个人数据保护风险评估 (PIA/DPIA)**

设置数据保护官 (DPO)　**嵌入式隐私保护 (PbD)**

- 独立监督
- DPA 接口人

供应商管理

个人数据泄露通知

- 通知监管机构 : 及时且不晚于 72 小时
- 风险较大的情况需及时通知数据主体

6 数据处理的合法性基础

- 数据主体的有效同意
- 为了履行合同所必要处理
- 为履行数据控制者法定义务所必要处理
- 为保护数据主体或他人重大利益所必更处理
- 为履行涉及公众利益任务所必要处理
- 为追求合法利益目的所必要处理，但不能影响数据主体基本权利和自由

7 个人数据处理七原则

- 合法、正当、透明
- 目的限制
- 数据最小化
- 准确性
- 存储期限最小化
- 完整性与保密性
- 可归责

8 个人数据跨境转移

充分性认定白名单

- 达到欧盟认可的充分个人数据保护水平的国家，如瑞士、新西兰等

标准合同条款

- 数据传出和传入方签署欧盟认可的标准数据传输协议并承诺遵守协议中规定的数据保护水平

其他

Privacy Shield 隐私盾协议

BCR

9 处罚

处以 1000 万欧元或全球营业额的 2% 的处罚

- 违反对数据控制者和处理者的要求，如 PbD、数据处理记录、安全保护、数据泄露通知、DPLA、DPO 等

在有些国家可能触发刑事责任 (监禁和罚款)

- 例如奥地利、德国、爱尔兰、丹麦等

处以 2000 万欧元或全球营业额的 4% 的处罚

- 违反数据处理基本原则，包括同意等
- 违反数据主体权利保障要求
- 违反跨境数据转移要求
- 未遵守监管机构的数据处理限制，拒绝执法调查等
- 违反各成员国法律基于 GDPR 授权规定的特定场景下数据处理要求

GDPR 法规解读

1 GDPR 的适用范围

- 在欧盟境内设有业务机构的组织，只要这些业务机构在欧盟境内的活动中处理个人数据。（属地）
- 如某一组织虽不在欧盟境内设立业务机构，但其处理行为：

(a) 发生在向欧盟内的数据主体提供商品或服务的过程中，无论此项商品或服务是否收费；或

(b) 对数据主体发生在欧盟内的行为进行监控，则也应当适用 GDPR。（属人）

2 GDPR 中的关键角色

- **数据控制者：**指单独或者与他人共同确定个人数据处理的目的、条件和手段的自然人、法人、公共机构、政府部门或其他机构。
- **数据处理者：**指代表数据控制者处理个人数据的自然人、法人、公共机构、政府部门或其他机构。

3 GDPR 数据主体权利

GDPR 中对于包括知情权、访问权、更正权、删除权（被遗忘权）、限制处理权、数据可携权、拒绝权、不受制于自动化决策权在内的权利进行了规定。

4 GDPR 个人数据处理七原则

原则	原则描述	合规解读	适用角色	
			数据控制者	数据处理者
合法、正当、透明	数据主体的个人数据应当以正当、合法、透明的方式被处理	个人数据、敏感数据、儿童数据、雇主数据 记录同意、撤回同意 正当性：提供信息（隐私通知） 透明性：提供信息的方式	✓	N/A
目的限制	个人数据应当基于具体、明确、合法的目的收集，不应以与此目的不相容的方式进一步处理	新目的合法性匿名化	✓	N/A
数据最小化	处理的个人数据应与处理数据的目的是适当、相关且必要的	充分、不超适度、必要	✓	N/A
准确性	个人数据应当是准确的，并在必要的情况下及时更新 根据数据处理的目的，采取合理的措施确保及时删除或修正不准确的个人数据	数据的准确性	✓	N/A
存储期最小化期限	存储个人数据不超过处理目的所必要的期限	留存、销毁方式	✓	N/A
完整性保密性	采取必要的技术或组织措施确保个人数据的适度安全，包括防止未授权或非法处理个人数据、数据丢失或毁损	风险评估、技术与组织措施、加密、化名、访问控制、监控数据泄漏	✓	✓
可归责	数据控制者需负责且能展示遵从上述原则	记录政策与流程、数据处理活动	✓	✓

5 GDPR 罚则

GDPR 中规定，违反对数据控制者和处理者的要求，如 PbD(Privacy by Design)、数据处理记录、安全保护、数据泄露通知、DPIA(Data Privacy Impact Assessment)、DPO(Data Protection Officer) 等，处以 1000 万欧元或上一年全球营业额的 2% 的处罚；而违反数据处理基本原则，包括同意等、违反数据主体权利保障要求、违反跨境数据转移要求、未遵守监管机构的数据处理限制，拒绝执法调查等或违反各成员国法律基于 GDPR 授权规定的特定场景下数据处理要求时，处以 2000 万欧元或高达上一年全球营业额的 4% 的处罚。所以，健康及生命科学企业需对 GDPR 合规予以高度重视，避免因违反 GDPR 合规要求而遭受到严重的经济损失。

GDPR 应对之道

1 公司层面

首先，在组织架构层面，普华永道帮助客户梳理和完善现有架构，例如数据保护官（DPO- Data Protection Officer）的设置，制定相关 KPI 以及完善组织和人员能力；其次，从合同条款层面，帮助客户拟定符合 GDPR 要求的相关条款及整改建议，除隐私政策外还包括中国和海外分公司间的数据跨境标准合同条款（ SCC – Standard Contractual Clauses ）、和第三方合作伙伴间的数据处理协议（DPA – Data Processing Addendum ）等，能够更好的约束和规范在 GDPR 要求下各自的权利和责任；最后，协助客户搭建完备的制度流程体系，包含将隐私保护融入研发流程（PbD - Privacy by Design）、设计应急响应规范等。

2 技术落地

普华永道基于 GDPR 的要求，结合亚马逊云科技的技术（相关技术详见“第四部分 亚马逊云科技的全球安全合规基础架构及网络服务”），协助客户识别云、管、端各系统 / 功能所收集的个人信息，通过个人信息影响评估（PIA）持续进行风险与合规分析，梳理数据全生命周期中的合规差距并提供技术落地方案：如加密传输 / 加密存储等。

为了更好地站在企业的角度梳理及明确合规义务，有条理、体系化地应对 GDPR 下新的合规工作，普华永道结合亚马逊云科技成熟的技术（相关技术详见“第四部分 亚马逊云科技的全球安全合规基础架构及网络服务”），从公司管理及系统落地两个层面帮助客户梳理以及解决业务场景下的合规风险。

2.2

美国关于健康数据管理的合规要求：HIPAA 和 HITECH

法规概要

HIPAA 和 HITECH 是美国关于健康数据管理的最重要法规。法案的颁布目的是为了更好地保护敏感的病人健康信息，防止在未经病人同意或知情的情况下披露，同时推动电子健康记录的使用。1996 年，美国卫生和公众服务部 (HHS) 制定了 HIPAA 关于隐私规则与安全规则，其下属机构 CMS 则制定其他 HIPAA 简化管理规则。此外，美国政府为了进一步推动电子健康记录（EHR）的使用、扩大数据泄露通知和受保护的电子健康信息的保护范围，美国前总统在 2009 年签署了《经济与临床健康信息技术法案》(HITECH)，加强了 HIPAA 关于隐私与安全的规定，并且明确对不合规行为设置了更严厉的处罚，以鼓励医疗保健组织及其业务伙伴遵守HIPAA隐私和安全规则。《图 3 HIPAA和HITECH架构关系》

图 3 HIPAA 和 HITECH 架构关系

法规解读

1 HIPAA 的受保护对象

HIPAA 中的隐私规则确立了国家标准，以保护病人的医疗记录和其他可单独识别的健康信息（统称为 " 受保护健康信息 "）。根据 HIPAA，受保护的健康信息被认为是与个人过去、现在或将来的健康状况有关的可识别的健康信息，这些信息是由 HIPAA 覆盖的实体创建、收集或传输，或由其维护，与提供医疗保健、支付医疗保健服务或用于医疗保健业务有关（PHI 医疗保健业务用途）。

2 HIPAA 的适用范围

隐私规则中还列出了十八类可以识别到个人的敏感信息。若要使记录符合反识别的标准，不再受 HIPAA 标准的约束。这些敏感信息必须从指定的记录中删除。十八类敏感信息如《图 4 HIPAA 敏感信息》，而 HIPAA 的适用范围则如 《图 5 HIPAA 适用范围》所示：

图 4 HIPAA 敏感信息

敏感信息

- 姓名或部分姓名
- 电子邮件地址的详细信息
- 与某人直接相关的日期
- 地理标识
- 电话号码详细信息
- 医疗记录编号
- 任何其他独特的识别特征
- 帐户详情
- 健康保险受益人号码
- 社会安全档案的详细信息
- 证书或执照号码
- 设备标识符和序列号
- 车辆牌照详情
- 网站网址
- IP 地址详情
- 指纹、视网膜和声纹
- 完整的面部或任何可比较的照片图
- 医疗信息

亚马逊云科技 | pwc 普华永道

图 5 HIPAA 适用范围

覆盖实体

- 健康计划，如各类个人及团体医疗保险；
- 医疗保健信息交流中心，如账单服务公司、重定价公司、社区卫生信息系统；
- 以电子方式提交 HIPAA 交易（如索赔）的医疗保健组织，如初级保健中心，专科诊所，医院等。

业务伙伴

- 第三方理赔处理机构；
- 医院聘请的个案管理顾问；
- 独立医疗转录员；
- 其法律服务需要接触到 PHI 的律师；
- 在电子医疗记录（EMR）内工作的 IT 顾问。

健康记录服务公司

- 开发、销售或提供个人健康记录服务的公司

3 HIPAA 的具体规则

HIPAA 法规具体可分为几个不同的规则，包括 HIPAA 隐私、HIPAA 安全、HITECH 和综合规则 (OMNIBUS Rules)，以及执行规则。所有覆盖实体和商业伙伴必须遵守所有 HIPAA 规则和条例。

a. 隐私规则

其中，隐私规则详细定义了何为受保护的健康信息，并对何种情况下这些信息可以被披露和使用做出了相关规定。该规则不仅明确了适用信息保护措施的适用范围，也明确了病人的个体权利，该规则的主要要求包括（但不限于）：

- 受保护的健康信息只有在得到病人授权的情况下才能向第三方披露，除非在法律允许的情况下（例如该披露与医疗保健治疗、医疗保健付款或医疗保健相关业务有关）；
- 即使满足了这些条件，不论情况如何，覆盖实体和业务伙伴必须遵守 " 最低必要规则 "（即为达到预期目的，提供最低限度的必要信息）；
- 每个病人都有权利检查和获得其记录副本，撤回之前的授权，并在档案不正确或不完整时，要求对其档案进行更正。

b.HIPAA 的安全规则

安全规则定义并规范了与受保护的电子健康信息的存储、访问和传输相关的标准、方法和程序，并且对患者未事先授权的患者信息使用做出了限制。硬件、软件和传输的风险分析和风险管理协议属于此规则的范畴。具体有以下几点要求：

- 覆盖实体应使用合理和适当的行政、技术和物理保护措施，以保护敏感电子健康信息的完整性和可用性；
- 作为其安全管理程序的一部分，覆盖实体应进行风险分析，具体措施主要包括（但不限于）：
  - 评估敏感电子健康信息潜在风险的可能性和影响；
  - 采用适当的安全措施以应对风险分析中确定的风险;
  - 记录所选择的安全措施，并根据实际需要，记录采取这些措施的理由；
  - 保持持续、合理和适当的安全保护措施；
  - 覆盖实体必须限制对其设施和电子设备的物理访问，同时确保允许授权访问；
  - 覆盖实体必须采取技术措施和程序，只允许授权人员访问存储或者传输中的受保护的电子健康信息；
  - 覆盖实体必须采取相关制度和程序，以确保敏感电子健康信息不被随意更改或销毁。

c. 交易规则：

本规则涉及 HIPAA 交易中使用的交易和代码集，包 括 ICD-9、ICD-10、HCPCS、CPT-3、CPT-4 和 NDC 代码。这些代码必须被正确使用，以确保医疗记录和受保护的健康信息的安全性和准确性。

d. 识别码规则：

HIPAA 对于使用 HIPAA 财务和管理交易的覆盖实体具有不同的识别码。HIPAA 要求医疗服务提供者需具备提供者识别码（NPI），以便在其管理事务中被识别。

e. 执行规则：

HIPAA 执行规则规定了对商业伙伴或覆盖实体的任何违规行为的处罚。这涉及到覆盖实体和业务伙伴的五个主要领域，包括 HIPAA 安全和隐私要求的应用、建立强制性的联邦隐私和安全漏洞报告要求、制定新的隐私要求和会计披露要求以及对销售和营销的限制、制定新的刑事和民事处罚和对违反 HIPAA 的执法方法，以及规定所有新的安全要求必须包含在所有业务伙伴合同中。

f.HIPAA 违规通知规则：

HIPAA 违规通知规则确立了数据泄露威胁到患者记录时应遵循的国家标准。该规则还涉及了另外两种违规行为：轻微违规和重大违约。

g. 综合规则：

- 有效地合并了如下四个独立的规则制定：
  - 对 HIPAA 隐私和安全规则要求的修正；
  - HIPAA 执行规则纳入了 HITECH 法案中规定的分级民事罚款结构；
  - 对数据泄露通知和处罚执行的进一步要求；
  - 批准有关 HITECH 法案违规通知规则的条例。
- 并具体规定如下内容：
  - 患者信息在营销中的使用管理；
  - 医疗机构报告被认为无害的数据泄露；
  - 确定商业伙伴和分包商要对自己的违规行为负责，并要求商业伙伴遵守 HIPAA；
  - 要求商业伙伴和分包商采用 HIPAA 隐私和安全要求。

4 HITECH 对 HIPAA 的补充

在 HIPAA 原有的违规通知规则和执行规则上做出了更严格的规定。

- **违规通知规则：**在 HITECH 法案颁布以前，业务伙伴没有保护受保护的健康信息的法律责任；当信息泄露发生时，如果受到影响的人数小于 500，则报告没有时间限制，只有人数大于 500 时，相关医疗服务提供机构和其他实体需要在 60 天内做出通告。
- **执行规则：**原先对不遵守 HIPAA 的经济处罚十分轻微，HITECH 扩展了 HIPAA 违规通知规则的适用范围，同时建立了违规行为分级制度，根据分级进一步加大了违规行为的处罚力度。
  - HITECH 将法律责任扩展到任何处理 PHI 或 ePHI 的实体。除此之外，HITECH 要求将任何没有安全补救措施的信息泄露情况告知病人。
  - HITECH 引入 " 违规分级制度 "，并对违规行为增加经济处罚。罚款金额增加（从每次违规罚款 100 美元到 50,000 美元，最高可达 150 万美元，并根据通货膨胀进行调整）使民权办公室（OCR）有更多的资源来追究不遵守规定的覆盖实体并执行 HIPAA。

5 HIPAA 与 GDPR 存在相似点与不同观点，本文对比两者的关键要求如下：

图 6 HIPAA vs. GDPR

HIPAA 和 GDPR 关键要求对比

	HIPAA		GDPR
适用范围	针对美国境内持有、处理或传输的受保护健康信息（包括非美国公民或居民）	<	处理欧盟个人数据
访问权	在信息维护期间，有权访问特定 PHI（即“指定记录集”的一部分）	<	访问所有已处理的欧盟个人数据的权利
数据可携权	必须以个人指定的方式导出数据（取决于相关实体的能力和安全措施）	>	必须以用户友好的格式导出和导入某些欧盟个人数据
更正权	有权更正某些 PHI（即“指定记录集”的一部分），但更正通常不涉及诊断等医疗信息	≈	有权更正所处理的欧盟个人数据错误
限制处理权	不涉及	<	有权撤回同意或以其他方式终止处理欧盟个人数据
终止第三方转移权	有权终止转移 PHI，除非与 HIPAA 的“允许用途”之一发生冲突	>	有权撤回同意对涉及特殊类别数据的次要目的的数据传输
删除权	无删除权	<	有权在某些情况下删除欧盟个人数据
同等服务与价格的权利	未明确要求	<	隐藏要求
私人诉讼权损害赔偿	无私人诉讼权	<	无上限
监管机构的执法及处罚	根据违规程度 - 每次违规（或每条记录）罚 100 至 50,000 美元，最高罚款为 150 万美元 / 年	<	上限为全球年收入的 4% 或 2000 万欧元，以较高者为准

< 范围小于　> 范围大于　≈ 范围相似

HIPAA HITECH 的应对之道

首先，从公司的治理及组织高层架构层面，定义一套包含清晰角色及义务的隐私及安全结构，以便公司的持续运营和协调运作。从政策及通知管理层面，协助客户梳理隐私政策、相关通知、披露及指导方针，确定其记录留存且适用现存法律法规。

从跨境数据策略层面，基于现行数据收集、使用和分享情况，计划跨境数据转移策略。从数据生命周期管理层面，帮助创建一个识别新的个人数据处理和使用活动的存续机制，并匹配适当的控制点。从个人权利处理流程层面，帮助确立有效的个人同意和数据主体请求流程，包括数据输入、限制、修改到会计披露。从信息安全层面，识别现行信息安全保护措施，并将相关安全控制与法律法规结合。

从培训及事前预防层面，帮助设计并执行相应的培训流程，建立企业层面的培训责任和角色义务。最后，帮助客户建立相应的流程控制体系，设计适当的应急响应规范。

通过 HIPAA 隐私及安全评估，普华永道为客户梳理流程控制点，并结合亚马逊云科技的领先技术（相关技术详见“第四部分 亚马逊云科技的全球安全合规基础架构及网络服务”），为方案的后续落地做铺垫。

图 7 普华永道的解决方案

普华永道 HIPAA 合规咨询方案

企业层面隐私及安全控制范围		询问
Strategy & Governance 策略及治理	Policy & Notice Management 政策及通知管理	[#] 会议访谈
Data Lifecycle Management 数据生命周期管理	Information Security 信息安全	
Individual Rights Processing 个人权利处理流程	Privacy Incident Management 隐私事件管理	检查
Third Party Risk Management 第三方风险管理	Training & Awareness 培训及预防意识	[#] 文档审阅

2.3

美国关于药品数据安全方面的合规要求：GxP

亚马逊云科技 | pwc 普华永道

良好实践规范（GxP）概要

GxP 一词囊括了多种与合规性相关的活动规范，指适用于制造和研发食品以及药物、医疗设备和医疗软件应用程序等医疗产品的生命科学企业或组织的法规和准则，例如，药品非临床研究质量管理规范 (GLP)、药品临床研究质量管理规范 (GCP) 和药品生产质量管理规范 (GMP) 等（图 8 GxP 构成体系）。总而言之，制定 GxP 要求的目的有两个：一是确保用于消费者的说明书和医疗产品的安全性，二是确保用于制定产品相关安全决策的数据的完整性。不同的国家 / 地区有不同的监管机构监督 GxP 质量管理体系的具体实施。在美国、欧盟、英国、日本等国家地区，GxP 是强制性的最佳实践规范。

图 8 GxP 构成体系

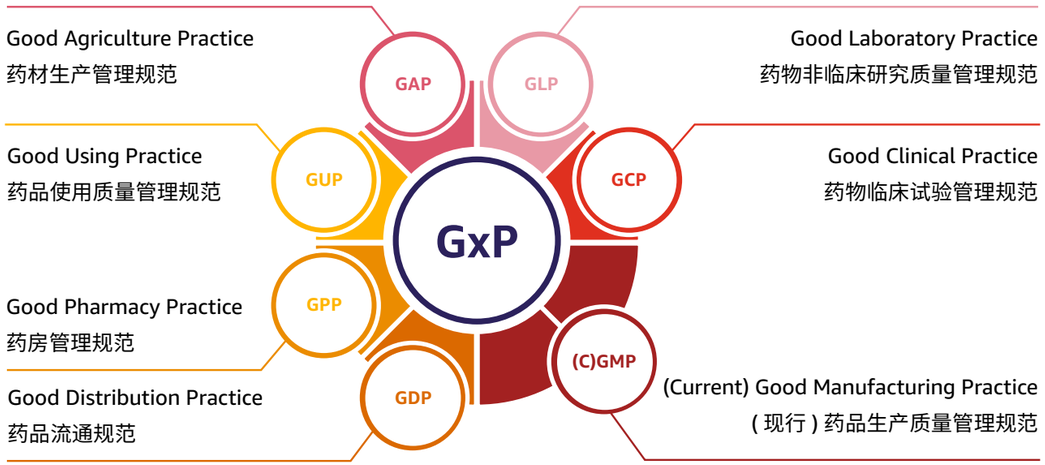


图 9 GXP 在美国法规的体现框架

以美国 GxP 为例，GxP 法规由美国食品和药物管理局 (FDA) 强制执行，并被纳入《美国联邦法规》第 21 章（以下简称“21 CFR”）。如《图 9 GXP 在美国法规的体现框架》所示：

GxP 解读

1 GxP 关于数据安全方面 (21 CFR Part 11)

美国食品药品管理局 (FDA) 颁布的 CFR 第 21 篇第 11 部分法规是 GxP 关于计算机系统安全性与电子记录方面的合规要求。“21 CFR Part 11”旨在允许受 FDA 管制的健康及生命科学企业或组织采用新信息技术，同时提供了一个框架，用于确保 GxP 电子数据可信且可靠。适用于涉及创建、修改、维护、存档、检索或传输的电子形式的任何记录，以便支持 GxP 管制活动。

“21 CFR Part 11”合规要求概要

要求	要求描述
有效性	• 验证系统以确保准确性、可靠性和一致的预期性能。
记录生成	• 能够以可读和电子形式生成准确完整的记录，以便机构能够进行检查、审查和复制。
审计追踪	• 使用安全的、计算机生成的、带时间戳的审计跟踪来独立记录操作员输入的日期和时间以及创建、修改或删除电子记录的操作。 • 系统中的所有过程都应记录在案，可追溯到特定的发起人，并具有相关的历史记录。此外，此历史记录应自动生成且不可修改。
运营管理	• 确保所有文件只由特定的个人审查，并确保它们在签署和开始临时阶段之前符合某些严格的要求。
安全控制	• 使用权限检查，以确保只有授权的个人才能使用系统、以电子方式签署记录、访问操作或计算机系统的输入或输出设备、更改记录或执行手头的操作。
培训	• 所有用户都必须接受必要的培训才能在系统中执行分配的任务和项目。
数字签名	• 数字签名是一种基于发起人身份验证的加密方法的电子签名，通过使用一组规则和一组参数进行计算，以便可以验证签名者的身份和数据完整性。 • 数字签名必须包括以下所有内容： ◦ 签字人的印刷体姓名 ◦ 应用签名的日期 / 时间 ◦ 电子签名的“含义”或意图

2 GxP 关于质量体系规范方面（21 CFR Part 820）

涉及美国食品药品管理局 (FDA) 根据 CFR 第 21 篇第 820 部分是 GxP 关于质量体系规范方面的合规要求，规定了所有医用器械成品在设计、制造、包装、标签、贮存、安装和服务中使用的方法，设施和控制。这些要求是为了确保医疗器械成品的安全和有效。

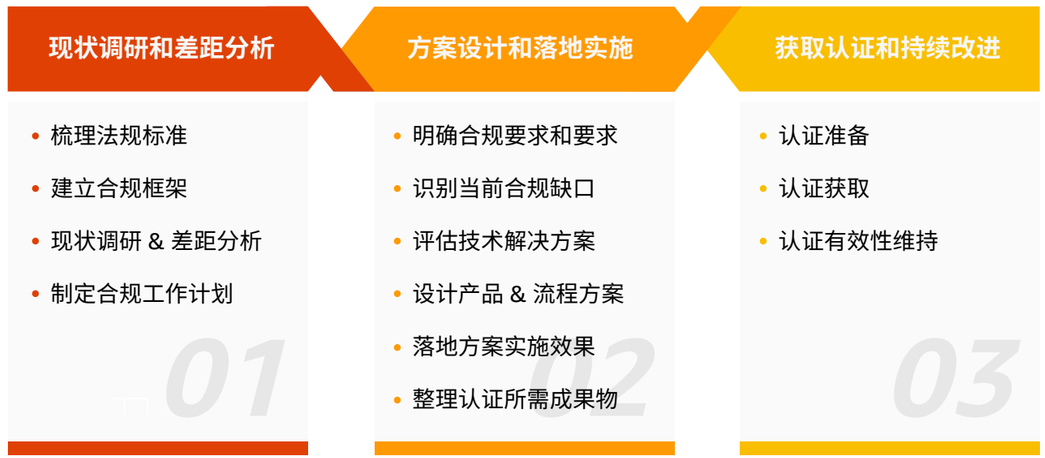
“21 CFR Part 820”合规要求概要：

要求	要求描述
质量体系要求	• 确保公司了解质量，制定质量体系程序和说明以实施和维护质量，定期审查质量管理体系并记录这些评审。 • 使用与合规医疗器械生产相称的组织结构，包括将适当的职责分配给适当的人员，并提供满足 FDA 要求所需的资源以及规划支持质量的实践、资源和活动。
设计控制	• 定期审查设计、开发计划以及设备（包括软件）以确保符合医疗设备的预期用途和用户需求。 • 计划和执行定期设计评审，其中包括参与评审功能的人员、未参与评审的人员以及专家。
文件控制	• 指定人员来查看和批准文档的更改。 • 以批准和分发文档相同的方式审阅文档更改。
采购控制	• 为第三方服务商设定质量要求。
识别与追溯	• 能够在接收、生产、分发和安装产品时识别产品。 • 能够识别失效时可能造成重大伤害的成品设备的单位和批次。 • 建立纠正措施程序，并记录可追溯性。
生产和过程控制	• 根据质量规范开发和监控制造设备的生产流程。 • 确保记录符合所需的控制措施，包括说明和标准操作程序。
验收程序	• 建立检查、测试或其他类型的验证程序。
不合格品	• 控制不合格产品，包括“标识、文件、评估、储存和处置”。 • 确定处置不合格产品的责任人、处置理由和处置流程的文件程序。
纠正和预防措施	• 在“过程、工作流程、许可、质检报告、质量记录、服务记录、投诉、退货和其他质量数据来源”中确定不合格产品质量问题的潜在原因
标签和包装控制	• 确保标签的完整性、准确性、可用性。
搬运、储存、分配和安装	• 制定搬运过程中所需遵循的程序，防止搬运过程中“混淆、损坏、变质、污染或其他不利影响”。 • 控制储存区域和储藏室，以防止“混淆、损坏、变质、污染或其他不利影响”，并防止意外使用“过时、拒收或变质的产品”。 • 控制设备的分发方式，只有批准分发的设备才能实际分发。审核采购订单并在分发前解决问题。 • 检查具有过期日期的设备是否已过期。保存分发记录。 • 为需要安装的设备创建安装和检查说明。确保安装人员正确安装并记录安装。
记录	• 将无需他人阅读的记录标记为机密，但 FDA 除外。 • 在设备的预期寿命内保留记录。

GxP 的应对之道

普华永道拥有经验丰富的项目团队，负责对整体质量体系执行评估合规缺口并设计制定合规解决方案，以及落地实施合规管治框架进而辅助企业获取认证和持续改进。普华永道专家能够协助企业解决质量体系合规风险所需的流程设计并促进可持续性实施程序。为了让健康及生命科学企业更系统、高效地应对合规标准，提升自身的信息系统管理水平和技术能力，普华永道建议企业在合规应对工作上分三步走。

图 10 普华永道的解决方案

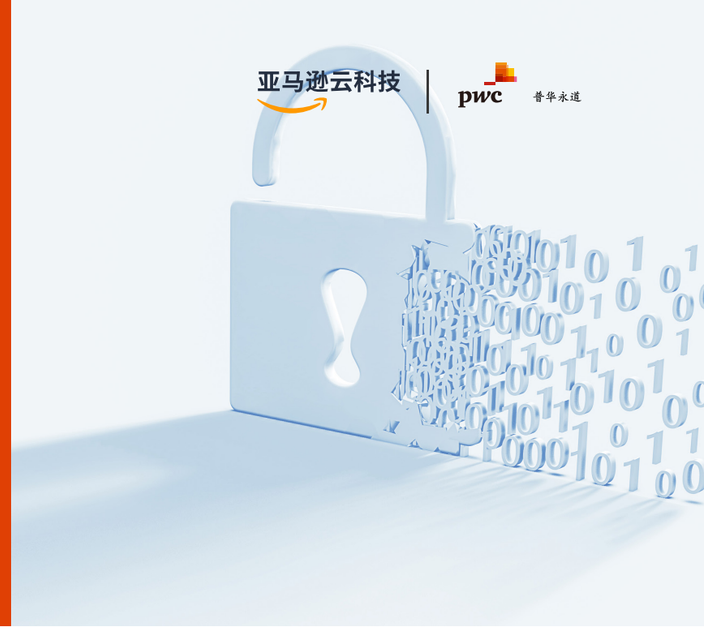


普华永道已建立的治理架构包括指导委员会提供监督和战略指导、跨职能多站点设计和实施团队、确定项目管理者和执行人员的角色以及建立定期会议时间表和沟通计划。在现状调研和差距分析阶段，对流程、人员和 IT 系统与监管标准和行业领先实体的差距进行评估，以确定它们是否符合相关行业标准，同时审核质量体系记录以进行充分的研究和制定纠正措施。

在方案设计阶段，定期举办重点小组研讨会，制定详细的系统路线图包括已定义的用户需求、功能需求和技术需求，制定流程设计的表单模板并收集反馈。在落地实施阶段，普华永道制定了全面的重新设计 / 补救计划，包括管理控制、设计控制、风险管理、供应商控制、生产和过程控制、投诉和培训。在获取认证和持续改进阶段，通过深度分析建立基线指标以跟踪趋势进展。当整合所有站点后随即进行有效性检查，建立阈值以标记改进和确定额外支持的需求，定期关注关键区域以跟踪进展并提供指导。

2.4

其他重要国家关于数据安全管理的合规要求



日本《个人信息保护法》(APPI) 概要

日本于 2003 年颁布了《个人信息保护法》(APPI)，以全方面地实现日本公民的个人信息保护。该法律旨在保护公民的个人数据免遭泄露，丢失或损坏；监督处理数据的员工；和托管数据的第三方监督，后多次修订，2020 年修订案将于 2022 年 4 月 1 日生效。修订案意在加强处罚，引入对某些违规行为的强制报告，加强 APPI 的域外应用，并扩大受 APPI 保护的数据的范围。

法规解读

1 APPI 的适用范围

APPI 区分个人信息和个人数据。“个人信息”(personal information)，是指属于下列情形之一的关于在世个人的信息：

- 通过该信息中包含的姓名、出生日期或其他描述可识别特定个人的信息，包括容易与其他信息对照后识别特定个人的信息；
- 含有个人识别符号（individual identification code）的信息，如驾驶证号码、护照号码等。

而“个人数据”（personal data），是指用以构成个人信息数据库等的个人信息。“个人信息数据库等”是指包含个人信息在内的信息的集合物，是通过检索可容易识别到特定个人的具有一定体系的信息集合物。

2 APPI 的受规范主体

APPI 适用于负责处理个人信息的所有经营者（个人和实体）。

个人信息处理者的范围

- 个人信息处理者

  “个人信息处理者”，是指将个人信息数据库等用于其经营业务的主体，但不包括国家机关等。
- 个人相关信息处理者
- 假名化加工信息处理者
- 匿名化加工信息处理者

对外国企业的适用

- 如果日本境外的个人信息处理者向日本境内自然人提供产品或服务，并因此取得日本境内自然人的个人信息、个人相关信息或由个人信息生成的假名化加工信息或匿名化加工信息后，在境外处理该等信息时，日本个人信息保护法的以下相关规定对取得及处理该等信息的行为同样适用，即有域外适用效力。

3 APPI 的主要内容

对个人信息处理行为的规范

个人信息处理者处理个人信息时，将适用以下各项规范：

- 正当取得个人信息；
- 明确特定使用目的；
- 取得个人信息时通知、公布使用目的；
- 禁止在特定使用目以外使用个人信息；
- 投诉的应对。

对个人数据处理行为的规范

个人信息处理者在处理个人数据时，除上述针对个人信息处理行为的规范以外，还适用以下规范：

- 使用个人数据的特定目的的公布；
- 确保数据内容的准确性；
- 安全管理措施；
- 个人信息处理者对其员工的监督；
- 个人信息处理者对受托方的监督；
- 向第三方提供个人数据的限制；
- 向境外第三方提供个人数据的限制；
- 向本人披露持有个人数据 (如姓名、年龄、ID)。

新加坡《个人数据保护法案》(PDPA) 概要

新加坡于 2012 年颁布了《个人数据保护法案》(PDPA)。该法案于 2014 年起生效，是一项用于在新加坡保护个人数据的法案，综合性规范了对个人数据的收集、使用和披露行为，保障了个人数据安全。

法规解读

1 PDPA 的适用范围

PDPA 适用的主体包括个人、公司、协会、社会团体等法人或非法人团体，无论该等自然人或实体是否依据新加坡法律设立，是否为新加坡居民或居民企业，或是否在新加坡具有办事处或营业地，只要以上自然人或实体具备以下数据处理行为，均适用 PDPA：

- 在新加坡处理个人信息，无论是新加坡 / 非新加坡居民个人信息；
- 处理新加坡居民个人信息。

2 数据控制者义务

义务类型	义务内容
同意义务	数据控制者收集、使用或披露个人数据之前，必须获得个人的同意
目的限制义务	数据控制者在适当的目的下收集、使用或披露个人数据
通知义务	数据控制者必须通知个人其收集、使用或披露个人数据的目的等
访问和更正义务	数据控制者应个人的要求，协助访问或更正个人数据
准确性义务	数据控制者必须做出合理的努力，确保数据的准确性
保护义务	数据控制者必须通过合理的安全安排保护其拥有或控制的个人数据
保留限制义务	数据控制者必须停止保留包含个人数据的文件，或删除个人数据，只要满足法定条件
数据转移限制义务	除非符合 PDPA 规定的情况，数据控制者不得将个人数据转移到新加坡以外的国家 / 地区
数据泄漏义务	对须予公布的数据泄露，数据控制者必须对已发生的数据泄露事件进行安全影响评估，并通知 PDPC 以及受影响的个人，但无论如何不得迟于评估后的 3 个自然日
问责义务	数据控制者必须执行必要的政策和程序，以履行其在 PDPA 下的义务，并应公开有关其政策和程序的信息，具体包括： 1．需任命数据保护官（Data Protection Officer）；2．需制定数据保护政策和实践

3 数据主体权利与保护

权利类型	数据主体权利
知情权	虽然 PDPA 没有独立的知情权，但 PDPA 规定的多项数据保护义务变相认可了知情权
访问权	数据控制者具有响应个人访问要求义务，例外情况下，数据控制者可拒绝响应
更正权	数据控制者具有响应个人更正要求义务，例外情况下，数据控制者可拒绝响应
删除权	PDPA 不赋予个人独立的删除权。但是，数据控制者具有法定的数据保留限制义务
撤回同意的权利	个人有权在发出合理通知的情况下随时撤回对收集、使用或披露其个人数据的同意
不受自动决策约束的权利	PDPA 不赋予个人不受仅基于自动处理的决定约束的权利
数据主体行权	1．如何提出行权要求（1）形式：书面；（2）内容：个人数据及该数据的使用、披露信息或更正要求；（3）方式：数据控制者提供或认可的业务联系信息。 2．响应时间要求 : 在合理时间内尽快响应个人请求，其认可的合理时间为 30 天。 3．费用 : 为响应申请人访问请求，可收取费用。

加拿大《个人信息保护及电子文档法案》(PIPEDA) 概要

《个人信息保护及电子文档法案》(PIPEDA) 作为一项加拿大联邦法案，在 2000 年通过后，于 2001 年开始生效。PIPEDA 主要规定了私人或者企业在进行商业活动时，使用个人信息时的范围与准则。适用于加拿大各省份中所有商业活动过程中对个人信息的收集、使用和披露，还适用于个人信息在国际以及省之间的传递。

法规解读

1 适用范围

PIPEDA 的规范对象是：(a) 在商业活动过程中从事信息采集、使用和披露相关作业的机构；或 (b) 在与联邦业务相关的运营中收集、使用或披露雇员或职位申请人的个人信息的机构，包括机场、飞机和航空公司、银行和授权的外国银行、省际或国际运输公司、电信公司、和广播和电视广播公司等。

该法案将“个人信息”定义为个人识别信息，将“业务联系信息”定义为用于与个人就其工作、业务或专业进行沟通或促进沟通的任何信息，包括姓名、职务、办公地址、办公电话等。法律描写的“商业活动”是指具有商业特征的常规活动、行为或特定交易，包括销售、换货、出租、会员活动、筹款等。

2 十项原则

PIPEDA 要求企业遵循 10 项公平信息原则来保护个人信息，其具体体现如下所示：

- 责任制原则；
- 确定采集和使用个人信息的目的原则；
- 当事人同意原则；
- 信息有限采集原则；
- 限制使用、披露和存储原则；
- 准确性原则；
- 安全保存原则；
- 获取过程公开透明原则；
- 当事人有知情权原则；
- 接受申诉并核实信息原则。

第三部分

行业合规前瞻

除了上述数据安全相关法律法规要求，健康及生命科学企业同时也应致力于提升合规模式，以应对各类除数据安全以外的合规挑战。普华永道发布的《医药行业合规未来展望》分析了医药行业合规的新兴趋势和商业影响，从战略、技术以及道德的角度讨论了行业合规所面临的挑战和优先事项，阐释了应如何有效规划合规职能，同时响应当前的业务需求。

《医药行业合规未来展望》中，将合规模式提升分为四个关键阶段，从最初建立合规活动开始，逐步发展成由道德和责任驱动的企业。1.0 阶段，即“财务驱动”，主要涉及基本控制的建立。2.0 阶段，即“法律和合规驱动”，标志着专门的合规职能的建立，包括任命合规负责人和确立汇报关系，使合规计划得以有效实施。行业中的合规领袖企业正准备进入 3.0 阶段，即“道德驱动”，这涉及商业、数字化和生物道德的合并。阶段 4.0，即“责任驱动”，代表了以全面的、道德的方式管理企业所提供的产品和服务，涵盖了可得性和定价决策，例如确定谁能以何种价格获得产品和服务。在这个阶段，责任是商业生态系统的重要组成。

目前，大多数健康及生命科学企业的合规职能处于 2.0 阶段，需要从根本上提升合规模式，达到合规 3.0/4.0 的阶段，未来发展道路和可以提升或增强的方向包括：合规团队的技能、文化和行为、环境、社会和治理（ESG）和企业社会责任（CSR）、技术及相关投资以及跨部门团队合作。以下重点介绍 ESG 和 CSR 以及技术及相关投资这两个方面。

1 提升环境、社会和治理（ESG）以及企业社会责任（CSR）

以下的例子体现了健康及生命科学企业如何从 ESG 和 CSR 角度来提升合规模式。

采取结构化的方法进行数据和生物伦理管理：企业采取三管齐下的方法，其一是建立数据和生物伦理宪章，例如规定在引进新系统时要符合的原则；其二是建立数字和生物伦理指导委员会，分别由首席数字官和首席医学官领导；其三是由跨职能的工作小组来支持这些委员会，以识别需要深入评估的主题，例如知情同意管理，并定期向高级管理层汇报。

精简可持续性管理数据的收集和报告并使之自动化：企业在开展可持续性相关的基线审阅和出具季度报告时，精简并自动化数据收集流程，关键数据指标包括温室气体排放水平、向商业伙伴提供的培训课程数量及商业法律案件的数量等。这一方法能帮助企业确定后续改进计划，并将手工或零散的信息收集转变为全面的数据驱动分析流程。

2 增加技术及相关投资

行业中的合规领袖企业正在致力于应对有关技术的风险与机会。

不少健康及生命科学企业将技术视为改变企业合规职能的关键驱动力。技术变革的飞速变化带来了挑战、风险和机遇。各类新技术发展的综合影响大大增加了风险水平。最重要的问题是，技术创新的速度通常超过任何法律和监管的变化，增加了舞弊的可能性。例如，技术发展使得利益冲突越来越难以察觉。

专注于通过自动化可以获得最大投资回报的领域：流程精简和自动化可以帮助相关团队腾出时间来参与流程的早期阶段，并主动提供战略上的前瞻性建议，而不是事后建议。

提升合规团队的技能：包括新增具备技术专业资格的人员，并提高当前团队成员的技能，更好地利用数据分析和智能技术，使他们能够将标准的人工程序自动化、风险动态可视化，专注于核心问题，并成为一个积极主动的商业伙伴。

第四部分

亚马逊云科技的全球安全合规基础架构及网络服务

4.1

亚马逊云科技的全球安全与隐私保护基础架构

亚马逊云科技致力于成为当今可用的最灵活和安全的云计算环境之一，安全已深深植根于我们的文化和流程，并渗透到我们所做的一切，我们将安全作为我们的‘Job Zero’，即安全是最高优先级的工作。作为亚马逊云科技的客户将会从为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益， 亚马逊云科技在安全基础设施之上提供的服务均有安全基线，客户无论规模大小均可基于亚马逊云科技强扩展性、高度可靠的基础设施和服务，快速、安全地部署应用程序和数据，开展云上业务创新。

4.1.1 亚马逊云科技“安全责任共担模型”

亚马逊云科技的“安全责任共担模型”，为云安全的建设设定了基本的原则。安全性和合规性是亚马逊云科技和客户的共同责任。亚马逊云科技负责“云本身的安全 ”，客户负责“云内部的安全”，亚马逊云科技会提供多层次的安全防护服务帮助提升客户云中的安全防护。亚马逊云科技通过“安全责任共担模型”降低了客户管理、运营底层基础设施的复杂性并节省了成本，同时为客户提供了部署需要的灵活性和控制力。

- 亚马逊云科技负责“云本身的安全”。 具体包括底层云基础设施和云服务，亚马逊云科技负责运行、管理和控制从主机操作系统和虚拟层到服务运营所在设施的物理设备以及提供的云服务的安全，这不仅降低了客户管理、运营底层基础设施安全合规的复杂性，按使用量付费的方式也帮助客户节省了成本。
- 客户负责“云内部的安全”，包括选用哪个区域、使用哪种服务、访问控制的授权、安全防护的手段等。客户的安全责任在使用亚马逊云科技不同服务时会有所不同。例如，客户使用 Amazon Elastic Compute Cloud (Amazon EC2) 服务，客户需要负责操作系统（包括更新和安全补丁）的管理、客户在实例上安装的任何应用程序软件或实用工具，以及每个实例上配置亚马逊云科技提供的防火墙（称为安全组）的配置。客户使用如 Amazon S3 和 Amazon DynamoDB，由亚马逊云科技运营基础设施层、操作系统和平台，而客户通过访问终端节点存储和检索数据，客户负责管理其数据（包括加密选项），对其资产进行分类，以及使用 IAM 工具分配适当的权限。

如今全球数百万客户选择亚马逊云科技，其中重要原因之一就是安全。亚马逊云科技安全合规的全球云基础设施及云服务是全球 190 多个国家 / 地区数百万客户选择亚马逊云科技的基础，其中包括金融服务提供商、医疗保健提供商和政府机构等，他们将一些最敏感的信息托付给我们，给予我们充分的信任。这种全球化的规模也让亚马逊云科技有机会看到更多的安全“异常“事件。亚马逊云科技快速地学习并解决这类异常，再将这种“鉴别安全异常和解决异常”的能力嵌入到亚马逊云科技的安全服务中，从而让更多的用户从中受益。真正做到从客户中来，到客户中去。

4.1.2 亚马逊云科技的全球安全

亚马逊云科技为客户提供完整的控制权 , 例如，我们全球基础架构的设计让客户 可以完全控制数据的物理存储位置，这可以帮助客户满足数据本地存储要求。 借助亚马逊云科技，客户知道谁在访问其内容，以及其组织在任何给定时刻消耗了哪些资源。 通过利用细粒度的身份和访问控制以及对近乎实时的安全信息的持续监控，确保其资源始终具有正确的访问级别——无论客户的信息存储在何处。 客户可以通过使用我们的活动监控服务来监测整个系统的配置更改和安全事件，甚至将我们的服务与客户现有的解决方案集成以帮助简化客户的操作和合规性报告，从而降低风险并实现增长。

通过亚马逊云科技，客户拥有自己的数据，控制其数据存储位置并控制谁可以访问这些数据。亚马逊云科技的服务对客户在账户中的客户数据处理保持透明，并且提供各种加密、删除和监控功能。

如需了解更多信息，请访问：aws.amazon.com/compliance/data-privacy-faq

4.1.3 用户的内容存储在哪里

亚马逊云科技数据中心建在世界各地的集群中。 我们将给定位置的每个数据中心集群称为一个亚马逊云科技的区域。 用户可以访问全球众多亚马逊云科技区域，并且可以选择使用一个亚马逊云科技区域、所有亚马逊云科技区域或多个亚马逊云科技区域的任意组合。 用户可以完全控制数据物理存储在哪个亚马逊云科技区域，这可以帮助用户满足合规性和数据本地存储要求。

4.2

亚马逊云科技云上的隐私保护

用户始终拥有自己的内容，包括对其进行加密、移动和管理保留的能力。 我们提供的工具可帮助用户轻松加密传输中和静态数据，以帮助确保只有授权用户才能访问这些数据。

亚马逊云科技提供很多安全服务，帮助客户实现云端的数据安全。这些服务涵盖身份与权限管理、数据保护与隐私、威胁检测与事件响应、风险管控及合规、响应与处置等几个方面。

4.2.1 身份与权限管理

亚马逊云科技为客户提供强大的身份管理和权限管理 ，确保适当的人员在适当的条件下有权访问适当的资源。亚马逊云科技提供了大量帮助客户管理用户身份及其权限的服务及功能，客户可以根据业务的需要，进行最小化的授权，并且对授权策略进行审核，以确保访问策略的安全性。重点服务：Amazon Identity and Access Management（“Amazon IAM”）以细颗粒度的身份认证与访问控制机制，结合对安全事件的持续监控和精准的安全权限设置，保障正确资源被相应正确人员访问。

通过 Amazon IAM, 客户还可以使用现有的身份验证系统 (如 Microsoft Active Directory) 向员工和应用程序授予对云管理控制台和云服务 API 的联合访问权限。使用任何支持 SAML 2.0 的身份管理解决方案都可以实现这类功能。

4.2.2 数据保护与隐私

亚马逊云科技数据保护服务提供加密、密钥管理和威胁检测功能，可以持续保护客户数据、监控和保护客户的账户和工作负载。亚马逊云科技使用很多不同的方法实施数据保护。其中，自动识别和分类数据可以帮助客户快速地根据合规的需要，发现并定位包括个人数据在内的敏感数据。Amazon Macie 使用机器学习技术并根据客户的配置来发现和保护客户的敏感数据并对其分类，可以识别个人可识别信息 (PII) 或知识产权之类的敏感数据，并为客户提供控制面板和警报，让客户了解此类数据的访问或移动方式。Amazon Key Management Service (Amazon KMS) 为客户提供数据加密，该服务深度集成于亚马逊云科技的 140 多项服务中，可帮助用户大幅减少人工操作，降低出错概率。对于数据保密要求更高的用户，还可使用 Amazon CloudHSM 来获得云上专属加密机服务。在数据计算过程中，用户可使用 Amazon Nitro Enclaves 的云端机密计算的技术，创建严密隔离的环境处理敏感数据。

针对传输中的数据，亚马逊云科技云上提供的 Amazon Certificate Manager（“ACM”）可帮助用户轻松地预置、管理和部署公有和私有安全套接字层 / 传输层安全性 (SSL/ TLS) 证书，以便用于亚马逊云科技服务和用户的内部互联资源。使用 ACM，用户无需再为购买、上传和续订 SSL/TLS 证书而经历耗时的手动流程。

4.2.3 威胁检测与事件响应

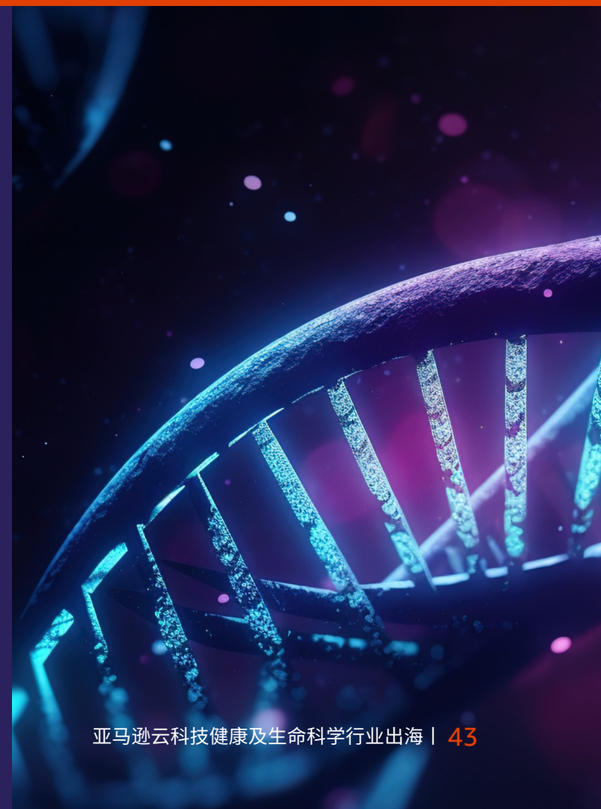
检测是安全生命周期的重要组成部分，可用于支持安全流程，还可以用于威胁识别和响应工作。客户使用检测服务和功能，可以识别潜在安全配置错误、威胁或意外行为。重点服务：威胁检测服务 Amazon GuardDuty 可持续监测恶意活动和未经授权的行为，该服务具有丰富的情报源并集成了机器学习的能力，可实现对威胁的精准定位，并对安全事件进行快速反应；Amazon Security Hub 安全事件统一管理平台为用户提供了一个统一的安全事件视图，并可根据不同的标准和最佳实践持续对用户的云环境进行合规性检查，快速发现技术差异并提供修复方案。

Amazon GuardDuty 是一种威胁检测服务，可持续监控恶意活动和未经授权的行为，从而保护用户的云账户、工作负载和在 Amazon S3 中存储的数据。迁移到云后，账户和网络活动的收集与聚合变得异常简单，但安全团队对事件日志数据进行持续的分析以发现潜 在的威胁，则可能十分耗时。Amazon GuardDuty 为用户提供了经济高效的智能选项，从而持续检测在亚马逊云科技中发生的威胁。

4.2.4 风险管控及合规

客户可以使用亚马逊云科技的自动合规性检查，持续监控其环境。例如，Amazon Artifact 自助门户，允许客户按需访问并免费获取亚马逊云科技的合规性报告。为避免用户在合规审计与评估中消耗过多成本，亚马逊云科技提供 Amazon Audit Manager，帮助持续审计客户在亚马逊云科技云上的资源和服务的使用情况，以简化评估风险；自动扫描、搜集证据，提供各种合规认证的模板，简化合规审计的证据收集工作，实现高效的自动化合规审计与评估；还能帮助用户管理利益相关者对用户的控件的审核，让用户能够创建审计就绪报告，且大幅减少手动操作。

客户还可以针对自己的特别业务要求完全自定义框架及其控件。基于用户所选择的框架，Amazon Audit Manager 会启动评估，持续从亚马逊云科技云账户和资源收集与整理相关证据，如资源配置快照、用户活动和合规性检查结果等。在管理控制台中启用框架后 Amazon Audit Manager 自动开始收集和整理证据。



4.2.5 响应与处置

Amazon Security Hub 可让用户全面查看亚马逊云科技云账户中的高优先级安全警报与合规性状态。客户可以任意使用一系列强大的安全工具，从防火墙和端点保护到漏洞和合规性扫描程序。借助 Amazon Security Hub, 客户现在可以设置单个位置，对来自多个云服务 (如 Amazon GuardDuty、Amazon Inspector 和 Amazon Macie) 以及来自合作伙伴解决方案的安全警报或检测结果进行聚合、组织和设置优先级。

Amazon Security Hub 的检测结果可在具有可操作图形和表格的集成控制面板上进行直观汇总。客户还可以使用自动合规性检查 (基于用户的组织遵守的亚马逊云科技安全最佳实践和行业标准)，持续监控用户的环境。Amazon Security Hub 的集成控制面板将所有账户的安全检测结果汇总起来，向用户显示当前的安全性与合规性状态。客户可以基于此采取必要的后续步骤。

4.3

亚马逊云科技云安全与隐私保护的最佳实践

亚马逊云科技云安全性基础设施致力于成为当今可用的最灵活和安全的云计算环境之一。它提供了一个可扩展性极强、高度可靠的云，允许客户快速安全地部署应用程序和数据。

亚马逊云科技客户将会从为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益。亚马逊云科技的一个优势是：客户可以利用亚马逊云科技进行扩展和创新，同时维持环境的安全。客户只需为使用的服务付费。与此同时，无论是从开源社区，还是生态合作伙伴，亚马逊云科技都能为不同的用户提供丰富的方案，可以让客户从更多样化的产品、方案中选择最适合自己的。

4.3.1 Landing Zone/ 着陆区云安全蓝图规划

亚马逊云科技的用户可以基于其企业组织架构、应用、开发、日志、管理等方面用亚马逊云科技 Landing Zone（登陆区）的最佳实践方法论构建一套云上最佳环境，从管理、数据、业务隔离等多个维度方面进行规范化的账号、权限和资源管控的设计。通过在首次上云时就按照最佳规范来指导所有业务人员和系统的配置，可以确保用户环境的整体一致性和最佳性能，这为构建夯实的客户自有的云平台打下了坚实的基础，并为后续基于云平台的业务的拓展提供了可靠的支撑。

Landing Zone 服务	Landing Zone 服务内容范围
亚马逊云科技账号与组织规划设计	OU，付费账号、安全账号、日志账号、生产账号、开发账号、测试账号，共享账号
身份访问管理设计	定义不同的用户组，角色，安全策略，用户组：Amazon Admin、Admin Linux/ Windows, Read Only, Operation Group, SecurityAuditor
VPC 网络设计	单 Region，测试、生产、共享服务共计 3 个 VPC，3 层子网结构设计
命名规范设计	子网命名、IGW、NAT、安全组、路由表等资源命名规范
日志集中管理设计	应用账号中的 Cloud trail、Cloud config、VPC Flow Log 存放在安全账号 s3 桶
云上安全服务设计	Config，CloudTrail, Security Hub，IAM 分析器，GuardDuty 服务
账号规划与实现	通过 Organization 构建亚马逊云科技账号结构
身份访问管理实现	自动化实现 IAM 用户角色及策略
VPC 网络实现	自动化实现 VPC 环境部署实现
日志集中管理实现	自动化多账号中的 Cloud trail、 Cloud config、VPC Flow Log 存放在安全账号 s3 桶
云上安全服务实现	自动化实现 Config，CloudTrail，Security Hub，IAM 分析器 GuardDuty 服务设定

亚马逊云科技的专业服务团队、专业的合作伙伴能够帮助用户完成 Landing Zone 的设计和实施。

4.3.2 Amazon Security Lake - 安全数据湖服务

Amazon Security Lake 自动将来自云、本地和自定义来源的安全数据集中到一个专门构建的数据湖中，存储在用户的账户中。借助 Security Lake，用户可以更全面地了解整个组织的安全数据。用户还可以改善对工作负载、应用程序和数据的保护。Security Lake 采用了开源标准 Open Cybersecurity Schema Framework（OCSF）。在 OCSF 的支持下，该服务可以规范和组合来自亚马逊云科技和各种企业安全数据来源的安全数据。

Amazon Security Lake

4.3.3 云上的自动化安全响应解决方案

此亚马逊云科技解决方案与 Amazon Security Hub 的一个附加组件，根据针对安全威胁的行业合规性标准和最佳实践提供预定义的响应和修复操作。它可帮助 Amazon Security Hub 客户在亚马逊云科技中处理常见的安全检测结果并改善自身的安全状况。其基于互联网安全中心 (CIS) 亚马逊云科技基金会基准版本 1.2.0、亚马逊云科技基础安全最佳实践 (AFSBP) 版本 1.0.0 的修复手册和支付卡行业数据安全标准 (PCI-DSS) v3.2.1 来构建修复手册，并可以实现自动化的修复。

4.3.4 基于亚马逊云科技安全合规基线方案

Prowler：https://github.com/prowler-cloud/prowler 是一款完全开源的项目，其基于亚马逊云科技安全最佳实践提供 240 项相关的安全扫描，并提供 CIS、ISO27001、GDPR、HIPAA 等最常见的安全合规评审项目。通过此开源方案，用户可以构建一套基于亚马逊云科技的内审平台，及时的了解环境的安全、合规运行状态。

基于 Porwler，目前亚马逊云科技提供：一键式部属的快速解决方案（Prowler - One Time Scan/OTS）和安全合规基线 Continue Compliance 两个免费方案，方便用户基于自身实际需求，快速上手使用。

4.3.5 网络

在如今全球化的时代，企业的业务会在世界各地进行开展，支撑开展全球业务的前提来自于对于全球所在地区的可触达、多样性的网络形式的接入、灵活的动态网络调整机制的全方位的支持。通过这些，IT 团队才能够更加快速的响应业务的全球化需求。由于中国大陆相关法律法规的要求，亚马逊云科技中国区域（由光环新网运营的北京区域和由西云数据运营的宁夏区域）与亚马逊云科技海外区域没有互联；因此下文中的部分网络类服务和功能在中国大陆区域的实现和可用性存在差异。

4.4

亚马逊云科技全球网络基础架构

4.4.1 全球区域覆盖

亚马逊云科技作为全球最大的云服务商，在全球主要的经济体：北美、南美、欧洲、亚洲、中东都有我们的物理区域覆盖，这些区域用于承载客户业务系统、计算、存储、数据处理等业务。截至到 2023 年 3 月，亚马逊云科技基础设施遍及 31 个地理区域的 99 个可用区，服务全球从初创公司，中小企业到大型企业和政府机构的数百万客户。通过亚马逊云科技的服务强化基础设施，提高敏捷性，降低成本，加快创新，提升竞争力，实现业务增长和成功。同时，亚马逊云科技还在不断规划和上线新的区域，用于更好的服务于各个区域的细分用户群。比如，即将上线的泰国区域就能够更好的服务这一东南亚的主要经济体和其周边的国家，如：越南等。

亚马逊云科技区域和可用区

即将发布区域：加拿大、以色列、马来西亚、新西兰和泰国新增 15 个可用区和 5 个区域。

4.4.2 自建全球骨干网络

为了提供高品质的网络传输体验，亚马逊云科技所有区域之间（除中国大陆与海外区域之间）都提供不少于双线 100Gbps 的带宽，使得用户可以完全利用亚马逊云科技的骨干网，以亚马逊云科技的区域为中心，构建一套可以服务于全球业务的网络架构。

亚马逊云科技还一直不遗余力投资、扩展、升级我们的骨干网，在过去的几年，我们分别新增了美国西海岸至日本、台湾、新加坡，美国西海岸至澳洲、新西兰，美国东海岸至英国、法国的海底光缆，为以后数年的亚马逊云科技的网络能力提供可靠的物理线路的基础性保障。

有关更多信息，请访问：

https://aws.amazon.com/cn/about-aws/global-infrastructure/

亚马逊云科技全球基础设施

亚马逊云科技区域，LOCAL ZONES，边缘站点，和全球骨干网

亚马逊云科技全球骨干网

- 冗余的 400 Gbps 线路
- 覆盖超过 245 个国家和地区
- 所有经过 Region, Local Zone 和边缘站点的流量都走骨干网

中国电信 CHINA TELECOM 世界触手可及

CTG Cross-Border VPC Connection (Asia Pacific:HongKong-China:Beijing)
By China Telecom Global
China Telecom Global ("CTG") ECP/Cloud Exchange is the service to improve the service performance of your applications for global users. By accelerating user access to applications, websites, and/or online platforms, ECP/Cloud Exchange enhances the work force of your cloud-based service. By leverag...

CTG Cross-Border VPC Connection (US East-China:Beijing)
By China Telecom Global Limited
China Telecom Global ("CTG") ECP/Cloud Exchange is the service to improve the service performance of your applications for global users. By accelerating user access to applications, websites, and/or online platforms, ECP/Cloud Exchange enhances the work force of your cloud-based service. By leverag..

CTG Cross-Border VPC Connection (US East-China:Ningxia)
By China Telecom Global Limited
China Telecom Global ("CTG") ECP/Cloud Exchange is the service to improve the service performance of your applications for global users. By accelerating user access to applications, websites, and/or online platforms, ECP/Cloud Exchange enhances the work force of your cloud-based service. By leverag...

CTG Cross-Border VPC Connection (Asia Pacific:Tokyo-China:Beijing)
By China Telecom Global
China Telecom Global ("CTG") ECP/Cloud Exchange is the service to improve the service performance of your applications for global users. By accelerating user access to applications, websites, and/or online platforms, ECP/Cloud Exchange enhances the work force of your cloud-based service. By leverag...

China unicom 中国联通

China Cross-border Direct Connection (ChinaDX-Asia)
By China Unicom Americas
China Unicom China Cross-border Direct Connection service, short name as ChinaDX, is an express cross China border AWS clouds inter-connection service to accelerate your cloud applications globally. By express connections of China AWS clouds with global AWS clouds, ChinaDX provides your express..

China Cross-border Direct Connection (ChinaDX Ningxia-Asia)
By China Unicom Americas
China Unicom China Cross-border Direct Connection service, short name as ChinaDX, is an express cross China border AWS clouds inter-connection service to accelerate your cloud applications globally. By express connections of China AWS clouds with global AWS clouds, ChinaDX provides your express...

4.4.3 基于亚马逊云科技构建跨境全球网络

亚马逊云科技截至目前在全球提供了 115 个用于专线连接 PoP 访问点，用户完全可以根据就近的原则，通过使用当地线路运营商提供的本地接入服务，快速构建起从 50Mbps 到 100Gbps 多种带宽的专线连接，将用户自有数据中心、办公机构进行高质量的互联，快速对接云上、云下业务。并且可以对接不同类型的网络接入请求，方便用户选择最适合自己的方式来构建覆盖全球的企业级网络。

4.4.4 构建安全合规的跨境网络（中国大陆区域与其他区域）

安全合规是我们对于用户秉承的最高标准要求，我们严格遵守中国大陆的相关法律法规，与有资质的跨境网络服务商合作，提供合规、安全和优质的跨境网络解决方案。根据中国法规的要求，中国大陆境内的亚马逊云科技区域（由光环新网运营的北京区域和由西云数据运营的宁夏区域）并没有和亚马逊云科技海外区域使用亚马逊云科技骨干网直接互联。用户可以自己向持有相关跨境专线资质的中国三大运营商采购跨境专线，将其在亚马逊云科技的海外区域的和其中国区域的虚拟私有云 (VPC) 使用私有连接进行互联互通。

为了提高用户开通跨境网络的效率，用户也可以通过亚马逊云科技海外区域的 Marketplace 直接在线申请三大运营商已经上线的的跨境线路服务；用户更可以通过订购不同运营商的跨境线路，构建多路高可用、全冗余连接，进一步提升网络通信的可靠性。

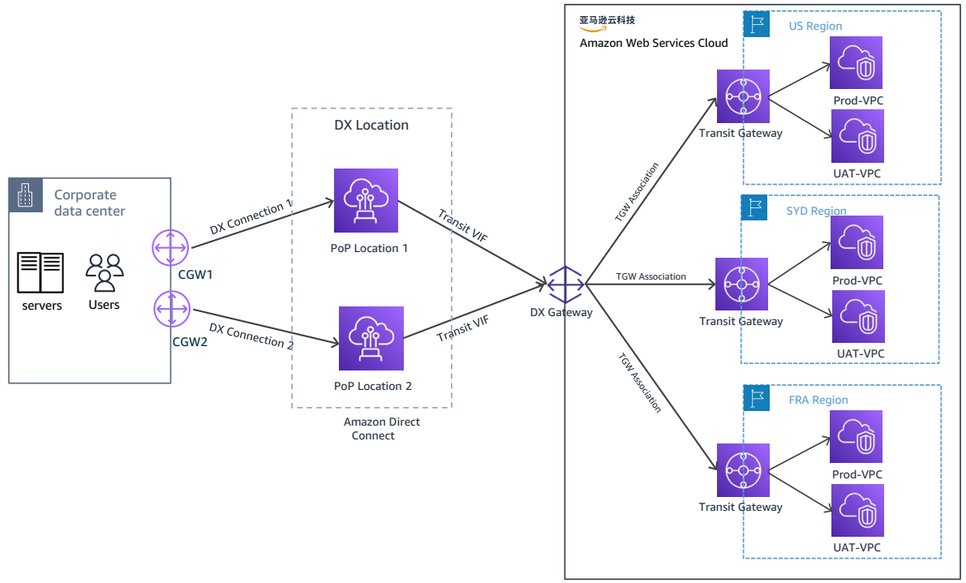
利用合规的专线和网络供应商，用户可以快速的构建从国内到海外的网络环境。

本地数据中心 / 办公室也可以通过三大运营商的专线服务将本地网络和亚马逊云科技海外区域打通，同时借助于 Direct Connect Gateway 服务实现一条专线 * 和全球多个区域网络打通，轻松实现全球网络连接和区域拓展。

* 用户必须在此跨境专线直接接入的亚马逊云科技海外区域有当地实体，且同时有使用该区域除专线以外的其他亚马逊云科技服务

对于业务可靠性、连续性有极高要求的用户，可以通过选择不同线路供应商的无路径重叠的物理线路，接入到不同的 Direct Connect PoP 点，以构建一套双活 / 高可用的客户自用跨境骨干线路，保证跨境业务连续性。基于亚马逊云科技 Direct Connect 的能力，用户可以让本地数据中心和亚马逊云科技云端的网络流量根据需要从指定的线路优先传输。当线路故障时，流量可以根据规则自动切换到另一根线路上，从而在网络层面提供极高的可靠性保障。

有关更多信息，请访问：https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html

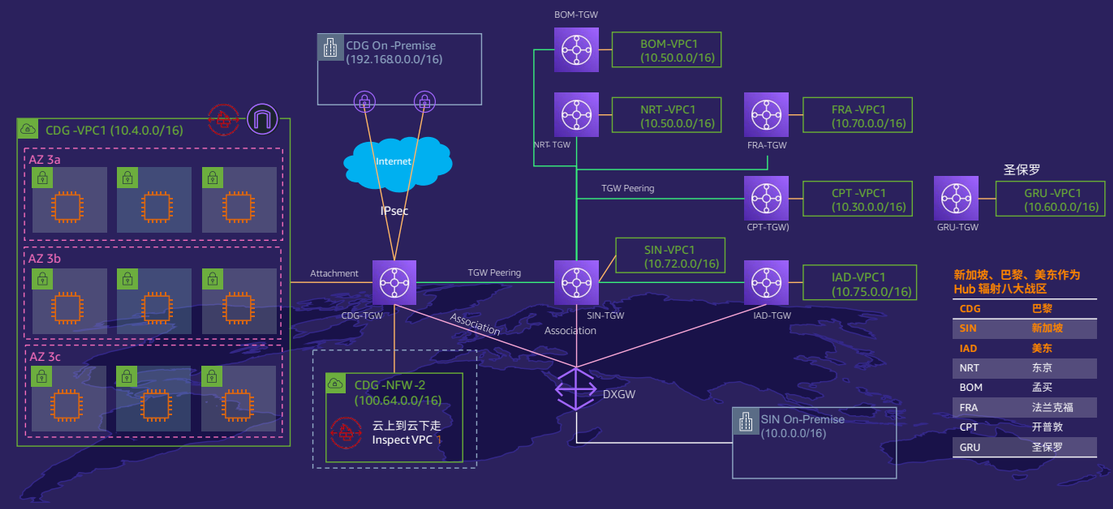


4.4.5 除亚马逊云科技中国区域外的全球组网

随着用户海外业务的不断扩展，其云上业务的多样性等需求会不断增加，如多账号、多区域、多 VPC、网络对等互联等需求会不断增多，这将会使全球网络的构建、运维变得极为复杂，且高昂的运维成本和复杂的管理给企业 IT 带来巨大挑战。

Amazon Transit Gateway 服务提供构建区域级别网络传输中心的能力，用户可用它来互连 VPC 和本地网络。Amazon Transit Gateway 充当一个高度可扩展的云端路由器，将多种连接方式（VPC, SD-WAN, Direct Connect, VPN 等）统一管理起来，极大简化了用户的网络设计、运维的复杂度。

利用TGW全球组网架构图



Amazon Cloud WAN 作为一种广域网 (WAN) 托管服务，提供了一个可视化中央控制面板，让用户可以跨区域轻松构建、管理和监控全球多个分支机构、数据中心及云端网络 (包括 Amazon Transit Gateway）。同时，Amazon Cloud WAN 可以基于网络规划快速生成用户的本地网络和亚马逊云科技云端网络的完整视图，以帮助用户监控网络健康状况、安全性和性能。用户还可以使用简单的网络策略来集中配置和自动执行网络管理和安全任务，并全面了解用户的全球网络。

4.4.6 高性能的最终用户访问

亚马逊云科技边缘服务可以在全球范围内以极低的网络延迟，安全地传输面向用户的数据。亚马逊云科技边缘服务主要包括有 Amazon CloudFront、Amazon Global Accelerator 和 Amazon Route 53，他们服务于亚马逊云科技在全球的每一个网络边缘，他们利用亚马逊云科技全球 100Gbps 的冗余光纤骨干网来加速数据的传输，为用户提供毫秒级网络延迟体验。

亚马逊云科技的全球边缘 PoP 在每个站点都有完整的亚马逊云科技边缘联网服务堆栈，以及缓存、网络连接、边缘计算和边界保护。目前亚马逊云科技一共提供 450+ 全球边缘 PoP（13 个区域缓存）以保证全球主要经济体所在地区的用户都能得到最佳的最终用户访问体验。

4.4.7 可自定义的内容分发网络服务

Amazon CloudFront 是一种全球内容分发网络服务，可以安全地以低延迟和高传输速度向浏览者分发数据、视频、应用程序和 API。450+ 全球边缘 PoP 将具有自动化网络映射和智能路由用于用户数据内容的分发，从而减少用户访问的延迟。 Amazon CloudFront 通过流量加密和访问控制提高安全性，并借助于 Amazon Shield 防御 DDoS 攻击，通过 Amazon Web Application Firewall(WAF) 构建应用防火墙以确保应用系统的安全，使用无服务器计算功能 Lambda@Edge 自定义用户在 Amazon Cloudfront 的边缘节点上运行的代码，以平衡成本、性能和安全性。

4.4.8 基于智能的 DNS 服务和基于 Anycast 任播网络的全球网络流量加速服务

Amazon Route 53 提供高度可用且可扩展的域名系统 (DNS)、域名注册和 Web 服务运行状况检查。使用分布在全球的域名系统（DNS）服务器，Amazon Route 53 将终端用户的域名解析请求可靠地路由到用户所指定的站点地址，同时 Amazon Route 53 可以根据网络条件自动从最优的节点进行相应的查询以获得最佳的查询效率。

Amazon Global Accelerator 是一种边缘服务，可以帮助客户提高供全球用户使用的应用程序的可用性和网络体验优化。Amazon Global Accelerator 可以轻松设置、配置和管理；通过提供的静态 Anycast 任播 IP 地址，为用户的应用程序提供固定的入口点，并消除了为不同亚马逊云科技区域和可用区管理特定 IP 地址的复杂性。IP 地址是来自亚马逊云科技静态任播地址，因此它们可以提供更靠近于用户的亚马逊云科技全球网络接入点，利用亚马逊云科技覆盖自建骨干网络，以更优的网络路径、更少的网络干扰来提升用户访问的速率。Amazon Global Accelerator 利用边缘的 TCP 终止将 API 工作负载最高提速 60%，并减少高达 40% 的丢包。实现一个站点服务全球访问的需求，而不必将应用程序部署到多个亚马逊云科技区域即可满足用户对高可用和最终用户访问服务的性能需求。

客户可以借助于 Amazon Route 53 智能 DNS 和 Amazon Global Accelerator 全球加速服务为最终用户提供最佳的前端到后端的访问体验。

第五部分

亚马逊云科技合作伙伴及 Marketplace

亚马逊云科技作为行业中领先的云平台服务商，为客户构建了行业中最完善的合作伙伴体系。 作为亚马逊云科技的客户，您可以通过这个体系，对接您所熟悉的合作伙伴并获取他们的解决方案，并且这些解决方案可以与亚马逊云科技的安全和合规服务无缝协作。

客户可以从亚马逊云科技的全球合作伙伴网络（“APN”）的技术和咨询合作伙伴列表中选择安全能力合作伙伴，他们专门为客户的特定工作负载和用例提供以安全为中心的解决方案和服务。

咨询和技术能力合作伙伴 Consulting and Technical Partners

Security engineering

8K Miles, accenture, AllCloud, >CMD Solutions, CLOUDZONE by matrix, CLOUDTEN, Deloitte., ECCOii, escala 24/7, FOGHORN, GUIDEPOINT SECURITY, HELECLOUD, Hewlett Packard Enterprise, Itoc, lightstream, logicworks, NRI, pwc, Smartronix Cloud Assured, Telefónica, VERSENT, direktgruppe, HITACHI Inspire the Next

Governance, risk, & compliance

Booz | Allen | Hamilton, Cloudyhuis, cavirin, CloudCheckr, CloudHealth by vmware, CloudPassage, COALFIRE, DivvyCloud, ECCOii, NTT DATA Services, KindlyOps, OPTIV, pwc, ScaleSec, Telos, TREND MICRO, Turbot, wirewheel, direktgruppe, stackArmor, KPMG

Security operations & automation

Cloudreach, ECCOii, Cloud valley, IBM Security, Mphasis The Next Applied, pwc, SAMSUNG SDS

同时，受益于 APN 合作伙伴解决方案提供的敏捷性、自动化和工作负载扩展，客户可以通过 Marketplace 轻松快速地查找、购买、部署和管理这些合作伙伴云解决方案。特别是在许多企业的在现有的管理体系中，网络安全流量控制和跨境组网等需求都需要专业的厂商和服务来满足企业的管理和合规要求。在这种情况下，客户可以利用亚马逊云科技提供的广泛产品和功能，也可以通过亚马逊云科技 Marketplace 服务轻松查找、购买、部署和管理构建解决方案所需的第三方软件和服务。

有关更多信息，请访问：

https://aws.amazon.com/marketplace/solutions/infrastructure-software/cloud-networking

aws.amazon.com/security/partner-solutions

aws.amazon.com/marketplace/solutions/security

第六部分

更多资源

亚马逊云科技 | pwc 普华永道

5.1 亚马逊云科技安全，网络及边缘加速相关产品主页

亚马逊云科技安全博客，了解最新的亚马逊云科技安全服务更新、发布和创新解决方案，aws.amazon.com/blogs/security.

亚马逊云科技网络博客，了解最新的亚马逊云科技网络、内容加速方面的服务更新、发布和创新解决方案，网址为：https://aws.amazon.com/blogs/networking-and-content-delivery/?nc1=h_ls

5.2 安全、身份和合规架构中心

通过文档、博客、视频和其他资源了解如何使用亚马逊云科技基础设施和服务来实现用户的安全和合规性目标。

https://aws.amazon.com/cn/architecture/security-identity-compliance

亚马逊云科技 GDPR 合规中心

https://aws.amazon.com/cn/compliance/gdpr-center/

亚马逊云科技 HIPAA 合规中心

https://aws.amazon.com/cn/compliance/hipaa-compliance/

亚马逊云科技 GxP 合规资源中心

https://aws.amazon.com/cn/health/solutions/gxp/

https://aws.amazon.com/cn/compliance/gxp-part-11-annex-11/

作者简介

普华永道中国

编写指导：

徐世达 | 普华永道中国内地及香港地区风险及控制服务市场主管合伙人

主编人员：

孙　燕 | 普华永道中国风险及控制服务副总监

叶玮慧 | 普华永道中国风险及控制服务经理

胡天泓 | 普华永道中国风险及控制服务

谈伊昀 | 普华永道中国风险及控制服务

孙　毅 | 普华永道中国风险及控制服务

亚马逊云科技

编写指导：

朱　翊 | 亚马逊云科技大中华区行业和解决方案部总经理

黄鹏飞 | 亚马逊云科技解决方案架构师团队经理

主编人员：

钱　凯 | 亚马逊云科技解决方案架构师经理

江学森 | 亚马逊云科技首席安全布道师

王熙明 | 亚马逊云科技网络服务产品团队经理

叶　明 | 亚马逊云科技边缘产品架构师

黄庆春 | 亚马逊云科技医疗及生命科学高级行业总监


亚马逊云科技
pwc
普华永道