



中国企业国际化进程中的 数字风险洞察报告

华信咨询设计研究院有限公司

2024 年 1 月

并购家 免费行业报告网

IPOIPO.CN 每日更新 不用注册会员 无广告 永久免费

版权声明

本报告版权属于华信咨询设计研究院有限公司，并受法律保护。转载、摘编或利用其他方式使用本报告文字或者观点的，应注明“来源：华信咨询设计研究院有限公司”。违反上述声明者，本公司将追究其相关法律责任。

前言

近年来，中国企业国际化进程加快，业务多元化趋势显著，各类型企业积极发掘国际市场机会。但同时，全球地缘政治竞争深入数字领域，数字博弈成为大国竞争常态，数字相关的风险在全球范围内迅速传播，对企业可持续经营造成较大的影响。在这一背景下，强化数字风险意识，提升数字风险防控水平，对于中国企业在国际化进程中实现可持续发展至关重要。

数字风险的多样性和复杂性，使得对其进行系统研究成为必要，但目前对数字风险的理论研究仍在探索中，对概念和分类尚未达成共识。通过对已有文献的广泛梳理，我们梳理了来自学术界和业界的最新见解，提出了企业国际化数字风险的分类体系，选取了三家中国企业作为研究标杆，调研梳理其应对数字风险的典型做法。最后，报告就如何提高企业在数字化国际化进程中应对数字风险的能力提出建议。我们期待通过这份报告为业界、学术界以及政策制定者提供分析、应对数字风险的视角和启示，共同推动中国企业在国际市场上的可持续发展。

目 录

前言

一、 研究背景	1
(一) 中国企业国际化进程加快	1
(二) 数字博弈成为大国竞争常态	2
(三) 数字风险成为中国企业国际化进程中的重要挑战	3
(四) 对数字风险的理论研究与实践应对尚不成熟	4
二、 中国企业国际化进程中数字风险的分类	5
(一) 外部环境相关数字风险	5
1. 数字监管风险	5
2. 数据法规风险	8
(二) 企业经营相关数字风险	8
1. 数字合规制度风险	8
2. 数字素养能力风险	10
(三) 技术应用相关数字风险	11
1. 数字基础设施风险	11
2. 数据信息安全风险	12
三、 中国企业应对国际化进程中数字风险的实践经验 ..	15
(一) 华为：强化数字风险防控组织保障	15
(二) 阿里巴巴：建设数据隐私及网安防护体系	17
(三) 吉利：健全业务合规管理体系	19
四、 提高中国企业数字风险应对能力的建议	22
(一) 强化公共关系管理，营造友好经营环境	22
(二) 提升经营管理水平，加强数字风险管控	22
(三) 培育人员数字能力，规避数字风险漏洞	24
(四) 关注信息安全保障，构建数字风险壁垒	25

一、研究背景

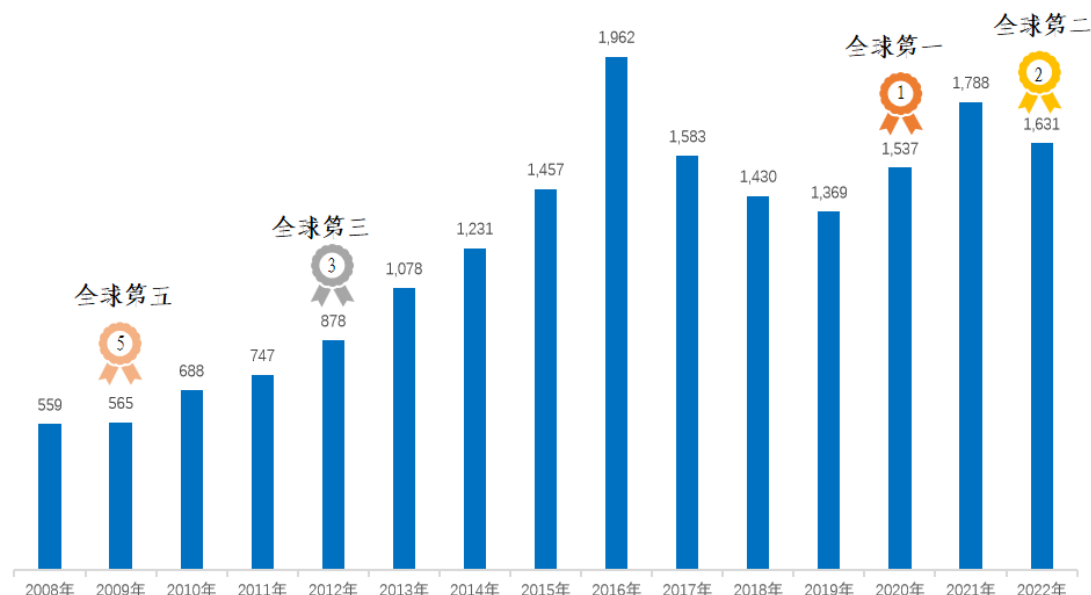
(一) 中国企业国际化进程加快

中国对外开放水平不断提升，多项国家政策引领企业出海。自 2001 年，中国共产党第十五届五中全会正式提出实施“走出去”战略，标志着中国鼓励性对外投资政策的形成¹。2013 年提出的“一带一路”战略持续引导中国企业出海。2022 年中央经济工作会议提出，坚持推进高水平对外开放是 2023 年经济工作的重点任务之一²。

在自身经营需求的驱使下，中国企业积极开拓海外市场。中国加入世贸组织后，国内竞争日益国际化，竞争空前激烈，迫使部分企业将目光投向国外市场，通过开展跨国经营和海外投资在国际市场上占有一席之地³。随着中国经济的快速崛起，越来越多的中国企业开始关注全球市场，大型企业及中小型企业都积极寻求跨国经营和海外投资的机会。

中国企业的出海战略更加多元化。在过去，企业主要以资源获取为核心目标，而如今更注重技术创新、品牌建设和市场拓展，积极参与沿线国家的基础设施建设、贸易合作和文化交流，形成全球化发展的新格局。实践证明，在全球化竞争中，一些中国企业已经成功实现国际品牌的

塑造，树立了良好的企业形象，为更深层次的全球合作奠定了基础。



*数据来源：商务部、国家统计局，国家外汇管理局

图 1 2008 年-2022 年中国对外直接投资流量（亿美元）

素材来源：开源信息整理

（二）数字博弈成为大国竞争常态

党的二十大报告指出，当前正处于世界百年未有之大变局之中。国际局势的变动主要体现为以中美博弈为代表的大国竞争，这一竞争涵盖了经济、科技等多个领域，深刻改变着全球地缘政治格局。中美之间的贸易争端潜在引发全球供应链的断裂和重新配置，给国际经济体系带来了巨大冲击。全球经济竞争也在科技创新、产业链布局等方面呈现出激烈的态势，尤其在人工智能、6G、量子计算等领域更为突出，主要表现在如下两个方面：首先，各国纷

纷投入巨额资金用于前沿数字技术的研发和应用，以保持领先地位。其次，数字博弈已逐步扩展至网络安全、全球舆情等多个层面，部分国家通过网络攻击、信息操纵等手段，试图在国际舆论场上占据主导地位，推动自身价值观和利益。再者，大国间数字博弈所带来的技术差距将进一步拉大数字鸿沟⁴，一些国家可能因为缺乏相应的技术基础和资源而被边缘化。

(三) 数字风险成为中国企业国际化进程中的重要挑战

全球数字化浪潮给风险的内涵和传播方式赋予了新的特征。全球数字经济增长速度快、发展潜力大，日益成为各国经济发展的重要动能和国民经济的重要支柱⁵。在此种背景下，风险的内涵和传播方式都发生了很大变化：与数字化因素强关联的风险将更快地在全球范围内传播蔓延，且将带来更多不确定性。

数字风险在全球范围内的传播更为迅速。全球数字环境互联互通的现状使得一个国家或组织的风险迅速传播到其他地区，例如某一地区的服务器瘫痪，可能立刻导致其他地区的相关服务不可访问等。

数字风险将带来更多的不确定性。数字化时代，由于企业、组织的业务和运营越来越依赖数字技术，信息的价值也随之增加，一旦发生信息泄露、数据破坏等风险，将

给企业和组织带来较大损失。

(四) 对数字风险的理论研究与实践应对尚不成熟

关于数字风险概念界定尚未达成共识。当前研究中明确提出数字风险概念并进行定义的文献十分有限，如陈伟（2021）及 Yadong Luo（2022）在研究中提出过相关定义。对数字风险的定义虽然未有普遍共识，但也有一些共同点，即与数字力量强相关的，或存在于数字领域的，对企业经营可能产生负面影响的不确定性。此外，对于数字风险的来源及分类研究成果较少且系统程度不高。

跨国经营的中国企业对数字风险的实践应对仍然处于探索之中。在全球重视数据安全的背景下，中国企业为应对不同国家的数据合规要求、处理日益严重的信息安全问题等，采取了开展专项合规工作、升级技术设备等解决方案，但对于跨国经营的数字风险尚无系统性分析，缺乏事前的研究与机制规划，更多的是亡羊补牢的被动操作。

二、中国企业国际化进程中数字风险的分类

数字风险的多样性和复杂性使得对其进行系统研究成为必要，但目前对数字风险的理论研究仍在探索中。通过对已有文献及企业实践的梳理，提出企业国际化数字风险的分类体系：根据风险来源，中国企业国际化经营面临着由外部环境、企业经营、企业技术应用引起的三大类、六小类数字风险。

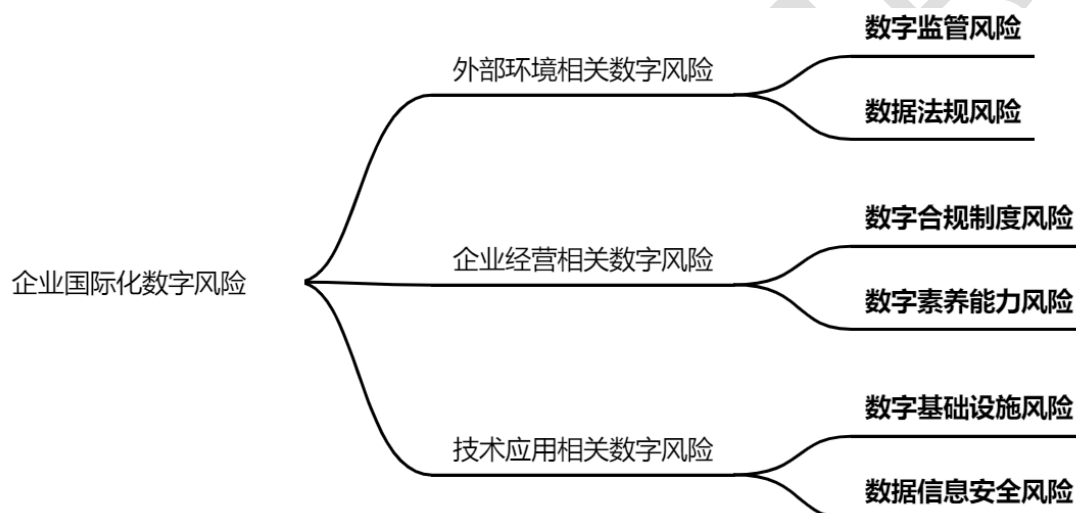


图 2 企业国际化经营数字风险的分类

(一) 外部环境相关数字风险

1. 数字监管风险

(1) 跨国数字制裁风险

此类风险指由于部分国家在泛数字领域对其他国家或特定个体和实施制裁，公司经营活动涉及被制裁区域、个体和实体，而对公司的经营产生的风险⁶。如美国以“涉嫌支持中国人民解放军现代化、影响美国利益”等理由⁷，将中国企

业列入商务部实体清单、国防部 CMCC 清单、财政部 NS-CMIC 清单等“黑名单”，从而对中国企业的数字服务采购、关键设备采购、产品出口、业务运营构成严重阻碍⁸。此类制裁常具有长臂管辖的特征，进入清单的企业不仅无法进口或使用美国的高技术产品和服务，且与第三国企业甚至一些中国企业的商业往来也被阻绝。例如，在没有美国许可的情况下，受制裁中国企业无法购买三星或台积电的高端芯片代工服务。

随着国际政治形势变化及全球技术竞争加剧，部分国家对中国在芯片和半导体、人工智能等领域的技术研发、国际合作等封锁逐渐升级，泛数字行业制裁与管制风险增加。

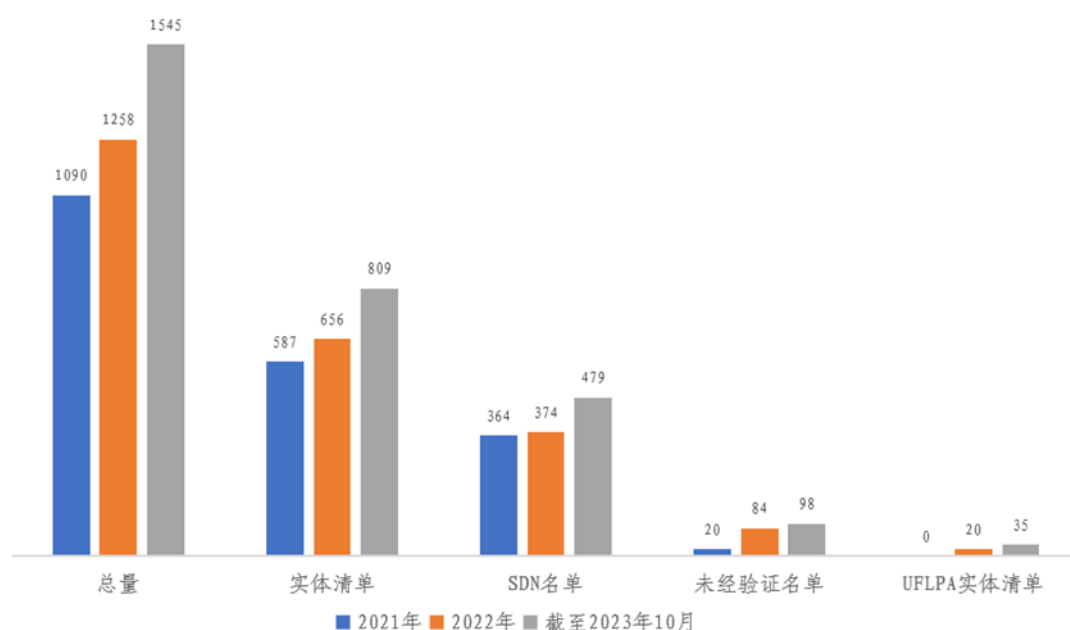


图 3 2021-2023 年被列入美国各“黑名单”的中国企业数

素材来源：开源信息整理

（2）东道国监管风险

此类风险指由于东道国政府出于本土企业保护、认知偏见等原因，对数字行业的企业采取更严格的行业监管措施，而导致企业业务运营、投资并购等方面受到影响。

为了维持本土企业的竞争优势，东道国可能对含中国企业在内的外国企业进行“选择性执法”。如英国援引《2021 年国家安全与投资法》叫停香港超橙控股收购总部位于英格兰的 Pulsic 公司，阻止中国企业获得高端集成电路开发相关的软件服务。又如，中国贸促会于 2023 年 3 月发布的《欧盟营商环境报告 2022/2023》表示，欧盟整体的营商环境恶化，在多个领域出台的保护主义政策工具，对外资企业提出了过度的合规要求，提高了外资企业进入欧盟市场的事前、事中、事后全过程的合规成本，中国企业在欧盟除了面对外资审查、外国补贴审查和公共采购审查外，还面临贸易救济措施的滥用。

此外，部分国家的政治舆论环境也容易造成数字执法偏见，中国企业常被部分海外政客、专家认为有义务将持有的所有信息和数据分享给中国政府，此种舆论倾向可能导致的行政措施，将对中国企业在当地获取、留存处理数据和信息，开展相关业务开展构成阻碍。

2. 数据法规风险

此类风险指由于全球各国的数据监管法规差异性大、法规内容不清晰、不同法规管辖范围分界不明显等原因，企业对数据法规研判不足，采取的数据处理措施不当，使得公司经营受到影响的情况。

不同国家和地区针对同一对象的政策和标准不同，将带来合规差异问题。如，在数据出域的规定方面，欧洲《通用数据保护条例》(GDPR)引入了以数据主体为核心的域外适用标准，而美国《澄清合法使用境外数据法》(CLOUD)则确立了以数据控制者为标准的域外数据管辖权，两类立法在域外适用过程中产生了直接的法律冲突⁹。此外，不同国家间的长臂管辖阻隔措施模糊，可能导致企业难以针对这些特殊性监管要求采取应对型的经营举措。例如俄罗斯于2015年颁布了《个人数据保护法》，印度于2018年提出了《个人数据保护法草案》，它们对数据处理行为的管辖范围不再局限于数据主体所在地，而更加关注数据处理行为是否在其管辖范围内发生¹⁰。

(二) 企业经营相关数字风险

1. 数字合规制度风险

此类风险指由于企业经营过程中数据合规审查、信息安全检查、内容审查等环节缺失或流程不畅，缺乏数字风险应

急应对机制等，导致企业在数据和信息管理上出现问题从而造成损失。

首先，缺少处理网络信息安全等数字风险的顶层设计，缺乏事件应对机制，是此类风险的原因之一。据调研，以典型国有企业为例，网络安全能力分散在各个部门、团队中，且缺少各业务间的联动与协作，难以满足安全保障需求¹¹。国资委《关于进一步加强中央企业网络安全工作的通知》指出，中国央企网络安全意识不强、重点防护不到位、监测预警能力不足、应急演练能力不够以及协作共享不充分等问题较为突出。

其次，在管理制度设计上，法律合规架构缺失、合规审查节点设置不合理等因素也是风险源之一。2021年《中国合规管理政策研究与国企合规管理调研报告》显示，仅有26%的国企成立了专门的合规管理部门。部分国企在重大经营决策或项目谈判过程中鲜有法律顾问参与，甚至未建立法律顾问参与制度，导致重要业务流程审查不严格¹²。此外，国企对海外子公司的合规违规追责方面，受机制设计缺陷和信息不对称的影响，执行力度较弱¹³。

第三，在业务经营过程中对数据和信息的操作不当，导致过度收集、越权收集信息和数据，也是此类风险的原因之一，多见于科技企业。若企业采集、留存远超业务经营所需

的信息，一旦发生泄露，将给被采集方和企业本身都带来更大损失。国家网信办于 2021 年组织对短视频、浏览器、求职招聘等 App 的个人信息收集使用情况进行了检测，发现抖音等 105 款 App 存在违法违规收集使用个人信息的问题。中国的《个人信息保护法》、欧盟的《通用数据保护条例》以及美国的《数据隐私和保护法案》等法律法规都规定企业及 App 应当最小化收集个人信息。

2. 数字素养能力风险

此类风险指由于专业人员缺失、信息安全意识不强、数字素养不高、责任心不强或团队设置不合理等原因，造成信息安全事故，从而给企业带来损失。人员在安全事件中始终扮演着非常重要的角色，Verizon 发布的《2023 年数据泄露调查报告》（DBIR）中指出，2022 年全球企业发生的信息安全事件中有 74% 涉及人为因素。

对于数字化人才的储备缺少预见性和主动性，人才储备不足的问题多见于国企。许多国企因忽视技术人才的培养和管理，面临着高职称技术人员锐减、中青年员工关键技术岗位“顶不上”的问题¹⁴，且许多国企受到行业限制和政策制约，难以向优秀技术人员提供与市场竞争力相匹配的薪酬和晋升通道¹⁵，企业内技术人员比例较低。根据万德数据库统计数据，2021 年在 486 家央企控股上市的公司中，技术人员的比

例仅为 22.2%，经营管理人员占比却高达 38.6%。

高管层缺乏数字风险应对的关键岗位设置，缺乏“牵头人”效应，也是此类风险的成因，中国企业普遍存在这一现象。数字化“牵头人”在宏观上预见预防潜在的安全隐患，同时还能够领导应对已经发生的安全问题，在企业职能序列中属于高管梯队¹⁶。例如，首席安全官多存在于外资企业中，而中国企业设置这一职位的情况不多见¹⁷，《中国首席安全官（CSO）调研报告》显示仅有 30.2%的中国政企机构设立首席安全官或相应级别岗位，近一半受调研的组织表示从未考虑过设置这一岗位。

数字素养缺失的问题在国企较为突出。培育和宣贯是提升数字素养的主要手段，但大型国企层级多，不可避免的会产生信息传递损耗，信息安全宣贯教育等也缺乏系统性，难以引发基层人员共鸣，宣贯教育效果不理想¹⁸。另外，国企信息安全建设注重引入技术产品，但忽略了提升管理能力和培养人员技能，安全技术的利用率和转化率较低¹⁹。

（三）技术应用相关数字风险

1. 数字基础设施风险

此类风险是指因东道国数字基础设施条件不足，例如云基础设施缺失、故障率高，通信技术落后、网络不稳定，硬件设备故障等，给企业运营造成损害的情况。

国际电信联盟研究显示，全球数字鸿沟问题依旧严峻²⁰，部分地区的数字基础设施薄弱、健壮度不足、老旧设备多，可用性存在问题，在此类地区开展业务可能面临 IDC 断电、故障等问题。许多国家的通信网络所处环境复杂，受各类自然灾害、人为破坏、战乱因素等影响的概率高，且基础网络运维不及时、不充分，容易导致网络大面积故障，使企业业务发生中断。最后，摄像头等物联网设备可能因为缺乏维护、系统补丁更新不及时等原因遭到入侵、破坏等，也构成此类风险。

2. 数据信息安全风险

此类风险指由于企业的 IT 系统建设不完备、数据平台相关的技术落后等原因导致数据、信息泄露和遭遇破坏，从而影响企业经营的情况。信息安全问题在数字化时代愈加凸显，因遭遇网络攻击、邮件钓鱼、自身上网规则不完备以及密码意外暴露等原因引发的信息安全事件，正在对全球企业产生深刻而广泛的影响，数据、信息的泄露和破坏已成为当前全球数据安全的主要挑战。IBM 发现，数据泄露给全球机构和企业造成的损失在 2020 至 2022 年间上涨近 13%，创下该年度报告发布 17 年以来的最高纪录²¹，近年来全球企业频遭木马、钓鱼邮件等技术手段攻击，数据信息泄露情况不容小觑。

企业如由于业务需要而频繁进行跨境数据传输，将显著提高数据和信息安全风险。不同业务类型的企业，由于跨境数据交互频率和规模、数据敏感程度等差异，面临不同程度的数据和信息安全风险。金融、科技等行业企业由于业务性质特殊，数据留存量大、信息流跨境交流密集，数据失窃、泄露、篡改、破坏等风险暴露程度明显高于业务信息流跨境少的传统企业。

IT 系统建设不完备，信息安全防护系统陈旧，补丁及技术解决方案未及时更新等原因，也将导致此类风险发生。企业在受到网络攻击、非法入侵和恶意破坏时无法有效应对，可能发生网络中断（拥塞）、系统瘫痪（异常）、数据泄露（丢失）、信息破坏等问题。随着全球经济数字化演进，跨国公司越来越容易受到恶意网络攻击，当前比较典型的网络犯罪包括消费者数据泄露、金融犯罪、市场操纵和知识产权盗窃等。黑客攻击和网络犯罪的方式也在演变和复杂化，从网络钓鱼、勒索软件到高级持续性威胁（APT），攻击者不断寻找新的漏洞和方式来侵入企业网络和系统。2017 年 5 月中国石油受到比特币勒索病毒波及，导致全国多个城市的加油站出现断网²²。2020 年至 2022 年，中国电信运营商、航空公司等由于部分骨干网络节点设备、核心业务系统服务器等被植入木马程序，内网和信息系统多次出现越权登录、数据外传等异常网

络行为²³。

中国企业自身拥有关键技术与设备知识产权的程度不足，也影响此类风险的发生。目前部分制造企业的工控系统和关键生产设备依赖其他企业，遇到突发情况运维得不到持续有效的保障，难以及时修复系统漏洞。此外，伴随国际局势不确定性与地区冲突升级，对华“制裁”举措常涉及科技领域，中国在智算、半导体、操作系统、EDA、数据库、办公软件、核心应用软件等细分领域对海外产品和服务存在一定依赖，一旦遭遇“制裁”，必然会影响以数据库和 ERP 为信息基础设施的信息系统安全。

三、中国企业应对国际化进程中数字风险的

实践经验

本文基于公开信息，从人员组织、技术应用及合规管理三个维度出发，梳理具有丰富出海经营经验、在应对数字风险方面有系统化举措的企业做法，供中国企业国际化业务经营借鉴。

（一）华为：强化数字风险防控组织保障

华为跨国经营业务的特点是敏感数据密集、对芯片等高端技术有较强依赖、全球业务分布较广、面临部分关键国家政治环境不友好等。其中：政治环境风险、数字化治理法规风险、政府监管审查风险、网络通信安全风险、信息及数据安全风险等问题较为突出，上述风险的典型应对方式之一是通过体系化的组织建设最大程度降低上述风险。

一是设立全球公共及政府事务部，加强对海外政策及政治环境的研判。华为在海内外多个城市均设有该事务部的办公室，作为面向政府、媒体、智库学者等利益相关人进行对话和沟通的窗口，并对所在海外市场所面临的数字风险进行量化分析和对标研究²⁴，为业务部门提供风险防控信息参考，也为战略部门提供研判全球风险的独家资料。

二是设立法务及合规团队，将审查节点全面嵌入业务流

程，预防业务经营中的数字风险。华为的法务及合规团队由合规专员、法律顾问和相关业务领域的专家组成，将控制点融入所有的业务流程，每个业务都需要经过法务部门的评审与签字。除了被动管理风险，其法务及合规团队还通过梳理公司业务所涉及的法律风险、法律环节及所需的法律支持，形成总体的风险视图²⁵，制定和实施合规政策、监督合规流程，并提供合规培训和指导，旨在确保公司在数据隐私保护、信息安全管理、反洗钱、反腐败等各个业务领域遵守相关的法规和政策要求²⁶。

三是成立网安团队，防控技术类数字风险。该团队由网络安全专家和工程师组成，负责监测和防范网络攻击、漏洞利用和其他潜在的网络安全威胁，同时开发和实施安全策略、进行网络安全评估和风险管理，并提供网络安全的咨询和支持。华为还拥有一支安全研究团队，致力于分析和研究最新的网络安全威胁、漏洞和攻击技术，他们与其他安全研究机构和行业合作伙伴保持紧密联系，共享安全情报和最佳实践，以提高产品和解决方案的安全性²⁷。

四是成立全球网络安全与用户隐私保护委员会，解决特定领域的风险。该组织作为公司最高级别的网络安全与隐私保护管理机构，负责决策和批准公司的整体网络安全与隐私保护战略。该委员会由全球网络安全与用户隐私保护官

(GSP0) 领导, 该角色负责领导团队制定网络安全与隐私保护战略和政策, 管理和监督网络安全与隐私保护在各个体系、各区域和全流程中的实施。这些措施有助于华为加强对网络安全与用户隐私保护的管理和落实²⁸。

(二) 阿里巴巴：建设数据隐私及网安防护体系

阿里巴巴集团的跨国业务特点是业务高度数字化、业务生态复杂、敏感数据密集、业务及数据流密度高、全球业务分布广、平台日访问量极大、遭遇的网络攻击密集等。其中：数字化治理法规风险、网络通信安全风险、信息及数据安全风险等问题较为突出, 主要通过数据隐私及网安防护体系建设应对上述风险。

集团安全部牵头打造安全体系。阿里巴巴集团安全部负责阿里巴巴集团的整体安全, 在安全基建、应用程序安全、数据安全、内容安全、智能风控、AI 安全与治理等多个方向持续投入, 在业务实战中打磨安全能力、沉淀安全模型、落地安全产品。阿里巴巴集团安全部与多所高校建立合作探索技术, 总结产业实践, 同时在全球多个大会上发表学术论文, 申报多项国际、国内技术发明专利²⁹, 具有丰富的理论和实践成果, 在国际上具有较强的影响力。

建设及时排障的高可用体系。为保障生产环境的稳定性及互联网金融系统的安全性, 阿里巴巴设置了网站可靠性工

程师（Site Reliability Engineer, SRE）团队，主要由研发、运维和测试人员组成，负责处理故障、保障网站稳定运行。阿里巴巴建设了一套高可用故障体系。由系统指标异常检测触发风险预警机制，允许 SRE 团队介入处理风险，实现“1 分钟发现, 5 分钟定位, 10 分钟恢复”的风险处置³⁰机制。

SRE 团队还成立专门的技术蓝军，用于发掘防御系统的弱点并发起真实的攻击。通过每周全栈级的技术攻防演练以及仿真环境模拟天灾人祸，考验技术架构的健壮性及技术人员的应急能力，从而提升系统稳定，实现系统的高可靠性和高可用性³¹。

制定分层的数据治理策略。结合数据类型、安全要求等级等因素，阿里巴巴将跨境业务分为区域化架构方案、隐私数据封闭方案和个人数据封闭方案。在区域化架构方案中，对数据进行无针对性隔离，同时针对按需过滤区域机房；在隐私数据封闭方案中，隔离各区域中的隐私数据，中心机房无区域非脱敏隐私数据；在个人数据封闭方案中，隔离各区域中的个人数据，中心机房无区域非脱敏隐私数据³²。

开展海外容灾基础设施部署。由于国内外基础设施条件不同，部分国家缺乏可靠的网络基建，可能会存在断光纤、断网等情况，因此需要构建能够全面覆盖基础设施并随时灵活调配资源的安全生产。为此，阿里巴巴在 IAAS 层搭建了涉

及全球 6 大区域、13 个物理机房、17 个逻辑机房 (AZ) 的海外数字商业基础设施，在享受弹性资源能力的同时却无需在多个国家、地区部署和维护数据中心；在 PAAS 层利用阿里云各类中间件、云产品进行全球部署，应对全球化进程中的系列技术挑战³³。

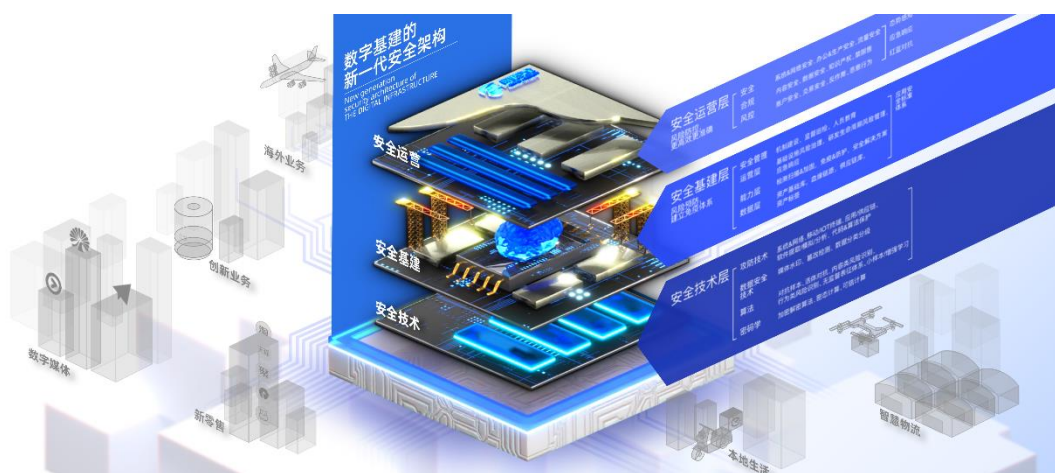


图 4 阿里巴巴安全架构

素材来源：阿里巴巴集团公司官网

(三) 吉利：健全业务合规管理体系

吉利集团迅速拓展海外市场过程中，全球业务分布广度随之扩大，其面临多样的数字化治理法规风险、信息及数据安全风险，主要通过业务合规管理实践应对上述风险。

建立分层次的合规制度体系。为适应海内外业务拓展的步伐，吉利集团参考联合国全球契约组织十项原则等国际公认准则及标准、国家相关部委合规管理指引和全球公司最佳实践，建立起清晰可行的四层合规制度体系，从准则到专项管理制度、指引及方法、操作工具，逐步实现各类合规风险

的管控。吉利所编制的《浙江吉利控股集团有限公司合规管理制度汇编》，包括合规行为准则、供应商行为准则 2 项准则，隐私保护合规管理制度、贸易管制合规管理制度等 6 项专项合规管理制度，合规风险管理办法、隐私保护合规管理机制建设指南等 10 项合规管理指引等内容³⁴，在数据隐私保护、跨境经营风险管控、数字合规风险预防方面起到了至关重要的作用。

持续推动数据及隐私合规保障。在数据合规方面，吉利于 2021 年起开展数据安全咨询和治理项目，识别、分类和分级数据资产，确保业务数据在整个数据生命周期中遵守相关的法律法规。此外，吉利还制定应用程序隐私合规指南，组织汽车网络安全和数据安全自检，检查吉利的所有应用程序以确保它们符合个人信息及隐私方面的合规要求。

强化出口及贸易管制相关的合规管理。为适应集团战略发展和运营管理需要，应对快速变化的国际环境和复杂形势，吉利成立了合规委员会，并下设出口及贸易管制合规专项工作组，该工作组负责审查落实解决出口和贸易管制合规重点专项工作，协调各业务合规团队建立出口管制和贸易合规多方联动沟通机制。合规部会定期开展合规培训，提高业务部门员工对出口和贸易管制合规风险意识和专业能力。

将合规工作成果纳入全球绩效评价。为强化合规管理，

防范合规风险，吉利制定《浙江吉利控股集团合规经营绩效评价办法（2022年版）》，并组织各下属业务单位开展年度合规经营绩效评价，定期检验合规管理工作的有效性，同时配合合规举报、合规文化建设、信息安全、商业伙伴合规等方式，实现合规风险闭环管理³⁵。

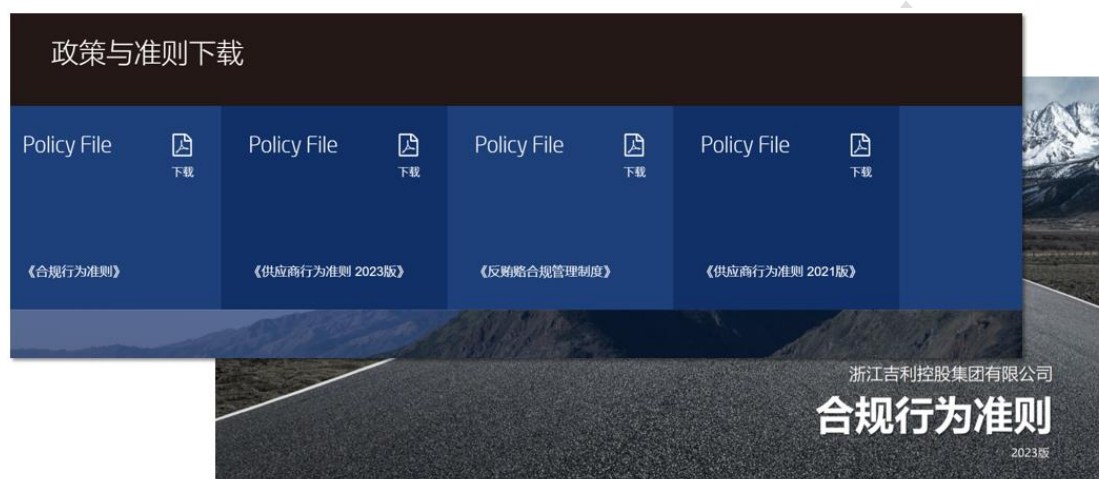


图 5 吉利全球隐私合规准则及政策

素材来源：吉利公司官网

四、提高中国企业数字风险应对能力的建议

(一) 强化公共关系管理，营造友好经营环境

维护与海外政府及媒体的关系，是有效应对外部环境相关数字风险的主要策略。中国企业面临着特殊的国际政治环境，需更加谨慎地做好对外沟通工作。

做好本地化政府关系工作。在每个海外市场设立专业的本地化政府关系团队，该团队不仅需要了解当地政治体系、法规，还要深入理解当地文化和社会动态，与当地政府和相关机构建立紧密的联系。这一职能条线的目的在于建立积极的合作关系，推动与当地政府的对话，使企业利益得到更好的保障。

建立紧急危机沟通计划。在数字风险事件发生前，企业应预先建立应对危机的沟通计划。确保企业在国际政治环境变动或出现风险事件时能够快速而有序地与当地政府进行沟通，及时防范潜在的负面影响，维护企业的声誉。

参与数字领域行业规则制定。拥有数字领域业务优势的企业应积极争取国际行业协会会员身份，参与所在行业的国际标准制定，组织、出席行业国际会议，打造全球影响力，提高自身产品与全球生态的兼容性。

(二) 提升经营管理水平，加强数字风险管控

企业应从战略、经营流程、合规等多个层面采取手段，

全面提升经营管理水平，防范数字风险。

在业务战略层面，应加强战略预研判，强化经营当地的信息同步。首先，企业应进行国际环境研究，明确在不同国家和地区的战略目标，制定相应的数字风险管理战略；应在各地建立信息同步的信息收集网络，实时获取本地政治、经济、法规等信息，设立定期的信息分享机制，确保总部和各地分支机构之间能够及时共享数字风险信息；在规划上，可根据所在行业、业务性质及国家政策等因素综合考量，对当地业务类型进行审慎选择，避免开展数字风险过高的业务。

在企业管理层面，建立完备的数字风险应对流程及机制。首先，应该结合当地及全球政治环境、企业业务类型、经营状况、技术水平、当地数字基建情况等，列出数字风险清单并制定预案。在进行海外业务流程设计时，应由合规与法务部门牵头，拉通市场、技术、人力、招采等各部门，将数字风险检查环节嵌入各个环节。在风险发生后，企业应立即按照预案召集由信息安全、法律、技术和公关等相关部门的代表组成的虚拟团队，评估和调查数字风险事件的性质、范围和影响，制定并执行相应的风险管控措施。

在法律合规层面，明确相应组织和职责，结合业务需求梳理法规领域的风险点，建立运行机制。首先，建立法务与合规职能团队，牵头组织公司的合规制度制定、日常业务检

查等工作，并对特别突出的数字风险领域开展专项行动。定期审查和解读适用于行业和地区的法规，确保对其有准确的理解，不断更新所在地法律动态库。各业务部门与职能部门合作，识别和梳理法律合规风险点。基于法规分析和风险评估，制定相应的合规策略，确保业务活动在法律框架内合法开展。将全球合规纳入公司的价值观中，通过领导者的示范行为和正面激励，培养员工对合规的认同和遵循，通过组织内部宣传活动帮助员工了解合规的重要性，宣贯法规要求和公司的合规政策。

(三) 培育人员数字能力，规避数字风险漏洞

企业应提升全体人员的风险意识，强化各条线员工的数字风险应对能力，打造具有数字风险识别及应对能力的人才队伍。

提升全体人员的数字风险防范意识。实施定期的数字风险培训，向全体员工普及数字风险的基本知识、最新威胁和应对策略。对近期较为密集的风险点进行定期推送，提高企业全体人员的警惕意识。定期组织数字风险演练，通过模拟真实场景，让员工了解如何在风险发生时迅速做出反应。

强化对关键岗位员工的数字风险培训。面向与客户数据、企业机密等敏感信息打交道的非技术岗位员工，提供数据隐私、合规政策、重点国家数字法规、全球政治环境等主题的

培训。针对可能成为社会工程攻击目标的员工开展专项工作，教育员工如何辨别和防范此类攻击。建立内部沟通渠道，鼓励员工分享数字风险防范的经验和最佳实践。

提升安全岗位员工的数字技术能力。在信息安全及网络安全团队配置具有专业背景的员工，确保团队能够深入理解和处理信息安全问题。通过外聘及外包等方式获取外部专家资源应对数字风险，尤其是安全专家、数据保护专家、威胁情报分析师、数字安全架构师等。

(四) 关注信息安全保障，构建数字风险壁垒

在信息安全领域，可以做好五方面的工作。

构建数据安全防护体系。部署高效的防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等网络安全设备，保障网络通信的安全性。在终端设备上采取端点保护措施，如反病毒软件、终端防护软件，以防范恶意软件和病毒攻击。对敏感数据采用加密技术，确保数据在传输和存储过程中的安全性，防范数据泄露风险。建立严格的访问控制机制，确保只有授权人员能够访问和修改敏感信息，减少内部威胁。实施定期的数据备份策略，并建立数据恢复机制，以应对可能的数据丢失或灾难事件。

强化信息安全管理能力。明确数字风险事故的责任划分，确保各个部门和岗位在数字安全事务中有清晰的责任和角

色定义，确保领导层、IT 团队、法务合规团队等关键部门对数字风险管理有统一的理解，并对各自的职责有清晰的认知。制定明确的信息安全政策，规范员工在处理数据和信息时的行为，确保公司整体的信息安全水平。部署实时监控系統，及时发现异常行为，建立紧急响应机制，迅速应对潜在的安全威胁。进行定期的安全审计，评估安全体系的有效性，并发现潜在的安全隐患。

加强关键数字资产的管理。根据敏感程度和合规性要求对数字资产进行分类和分级，对于高敏感的数据，应优先考虑在东道国建立本地存储设施，或选用合适的云服务商，仅在必要情况下跨境传输数据，并使用技术手段减少数据跨境传输过程中的风险，确保数据的获取、留存、使用、删除的安全性与合规性。

加强硬件设备的管理。建立全面的硬件设备清单并及时更新，内容包括服务器、网络设备、终端设备等，记录每个设备的型号、制造商、关键配置和责任人信息。制定硬件设备采购规范，确保购买的设备符合安全性和性能要求。建立定期的设备维护计划，包括固件和软件升级、漏洞修复、硬件巡检等，确保设备的正常运行和安全性。设立物理访问控制策略，限制对关键设备的物理访问。只有经过授权的人员才能进入设备房间或机房。部署设备监控系统，实时监测设

备的状态、性能和异常情况。启用设备的日志记录功能，记录设备的操作、事件和异常，便于事后溯源和分析。

做好数字基础设施灾备。制定数字基础设施灾备计划，明确关键设备在灾难事件中的备份和恢复策略。实施定期的灾备演练，验证数字基础设施灾备计划的可行性，及时发现和纠正潜在问题。与供应商签订技术支持和服务合同，确保在出现故障时能够及时获得支持和维修。在网络架构中实施隔离措施，防范网络攻击对关键设备的威胁。

参考文献

- [1] 刘建丽. 国企国际化 40 年: 发展历程及其制度逻辑[J]. 经济与管理研究, 2018, 39 (10): 13-30. DOI: 10.13502/j.cnki.issn1000-7636. 2018. 10. 002.
- [2] 杨立强. 中国中小企业“走出去”的基础与策略研究[D]. 对外经济贸易大学, 2003.
- [3] 张旭, 郭义盟. 中国国企国际化的时代背景、发展历程与世界意义[J]. 理论学刊, 2021 (02): 79-89. DOI: 10.14110/j.cnki.cn-37-1059/d. 2021. 02. 009.
- [4] 贾平凡. 美国霸权危害全球“数字人权”(环球热点)[N]. 人民日报海外版, 2022-09-01 (6).
- [5] 中国信息通信研究院. 全球数字经济白皮书(2023 年)[R]. 北京: 中国信息通信研究院, 2023.
- [6] 张心志, 唐巧盈. 拜登政府的芯片产业政策——复合困境与发展趋势[J]. 国际展望, 2023, 15 (03): 95-114+156. DOI: 10.13851/j.cnki.gjzw. 202303006.
- [7] 网易号. 美制裁 6 家中企后, 2 大国企退出亚欧互联网光缆项目, 撤资 6.8 亿元[EB/OL]. 2023[2023-09-22]. <https://www.163.com/dy/article/HTC621R605539IG6.html>.
- [8] 华麓管理咨询. 美国黑名单上的中国实体猛增至 1110 家 | 附中英文完整清单[EB/OL]. 2023[2023-09-22]. <https://mp.weixin.qq.com/s/TY2KZWgH2TWg7-iGLkcRWw>.
- [9] 王燕. 数据法域外适用及其冲突与应对——以欧盟《通用数据保护条例》与美国《澄清域外合法使用数据法》为例[J]. 比较法研究, 2023 (01): 187-200.

[10] 齐鹏. “一带一路”数字经济数据跨境风险的系统性应对逻辑[J]. 西安交通大学学报(社会科学版), 2021, 41(05): 104-113. DOI: 10.15896/j.xjtuskxb.202105011.

[11] 熊宁. 国企数字化转型中的网络安全防护与保密管理[J]. 网络安全技术与应用, 2021(07): 118-119.

[12] 刘岚. 新时代国企法律风险防范研究[J]. 法制博览, 2022(16): 148-150.

[13] 杨莹. 优化合规管理的四大体系[EB/OL]. 2019[2023-09-22]. <https://mp.weixin.qq.com/s/rMVq16SU0pk7S-tIYL-oAw>.

[14] 周文斌, 李宁, 唐华茂. 新时代人才强国战略下国企人才队伍建设研究[J]. 企业经济, 2023, 42(04): 16-27. DOI: 10.13529/j.cnki.enterprise.economy.2023.04.002.

[15] 李阳朔. 国企建设高质量人才队伍的策略探析[J]. 中小企业管理与科技, 2023(12): 97-99.

[16] 段玉强. 浅探中国企业实施 CSO 的必然性[J]. 沿海企业与科技, 2005(10): 28-29.

[17] 李建平. 信息安全重新定义首席安全官[J]. 中国信息安全, 2021(11): 36-39.

[18] 陈剑飞, 王小亮, 徐明伟. 大型国企网络安全宣贯教育工作浅析[J]. 中国信息安全, 2022(01): 43-45.

[19] 安永 EY. 国资智汇 | 数字化浪潮下国企网络安全管理战略转型[EB/OL]. 2023[2023-09-22]. <https://mp.weixin.qq.com/s/QdAUvtGBdZz5JQQXb14I5g>.

[20] 联合国. 联合国会议呼吁在最不发达国家实现更包容和公平的数字转型[EB/OL]. 2023[2023-09-22]. <https://news.un.org/zh/story/2023/03/1115852>.

[21] IBM. 2022 年数据泄露成本报告 [EB/OL]. 2022 [2023-09-22]. https://www.ibm.com/reports/data-breach?_gl=1*wnk6db*_ga*MjExMzcwMjc1LjE2ODUzNDQ2NTA.*_ga_FYECCCS21D*MTY5NTcwOTgyNy4yLjEuMTY5NTcwOTkxNC4wLjAuMA...

[22] 环球网. 中石油受勒索病毒波及 超 8 成加油站已重新连网 [EB/OL]. 2023 [2023-09-22].
<https://finance.huanqiu.com/article/9CaKrnK2L2y>.

[23] 安全内参. 年度盘点: 2022 年我国重大网络攻击事件 [EB/OL]. 2022 [2023-09-22].
<https://www.secrss.com/articles/50568>.

[24] 罗彪. 洞察: “神秘”的华为公共及政府事务部是何种存在? [EB/OL]. 2020 [2023-09-22].
<https://xueqiu.com/7367224626/148860502>.

[25] Techlaw. 华为法务部的战略定位与合规实践 [EB/OL]. 2019 [2023-09-22].
<https://mp.weixin.qq.com/s/QAZsxeUdapFu5owG-QEzZA>.

[26] 华为官网. 合规与诚信 [EB/OL]. [2023-09-22].
<https://www.huawei.com/cn/compliance>.

[27] 未然实验室. 未然实验室 “防患于未然”, 立体呈现华为安全主动防御体系 [EB/OL]. 2017 [2023-09-22].
<https://mp.weixin.qq.com/s/Euj4e50c8-zAr4Sti0-6nQ>.

[28] 华为官网. 网络安全与隐私保护 [EB/OL]. [2023-09-22].
<https://www.huawei.com/cn/compliance/cyber-security>.

[29] 阿里巴巴集团. 阿里安全的技术实力 [EB/OL]. [2023-09-27]. <https://s.alibaba.com/technology>.

[30] 悟鹏. 这是阿里技术专家对 SRE 和稳定性保障的理解 [EB/OL]. 2021 [2023-09-22].

<https://mp.weixin.qq.com/s/DUfoMeJa0spH00d1p0RSdQ>.

[31] 蚂蚁金服科技. 听说支付宝有一个“疯起来连自己都打”的项目 [EB/OL]. 2018 [2023-09-22].

<https://mp.weixin.qq.com/s/8XpJa75cH1e61kRGI3Af1w>.

[32] 阿里技术. 6 年技术迭代, 一文详解阿里全球化出海&合规的挑战及探索 [EB/OL]. 2022 [2023-09-22].

<https://www.infoq.cn/article/2fBuWxxkR1EkFj0Spihw>.

[33] 李伟杰. 6 年技术迭代, 阿里全球化出海&合规的挑战和探索 [EB/OL]. 2022 [2023-09-22].

<https://www.jiqizhixin.com/articles/2022-07-01-6>.

[34] 汽车预言家. 【吉利“飘”绿 ①】: 由内向外的变革 [EB/OL]. 2023 [2023-09-22].

<https://zhuanlan.zhihu.com/p/635234478>.

[35] 澎湃新闻. 清廉民企 | 吉利: 嫁接跨国公司经验和成果, 成为民企合规管理样板 [EB/OL]. 2020 [2023-09-22].

https://www.thepaper.cn/newsDetail_forward_10604586.

关于作者

编写人

余沐阳，华信咨询设计研究院有限公司咨询院研究中心
咨询顾问

李兴腾，华信咨询设计研究院有限公司博士后研究员

审核人

赵学健，华信咨询设计研究院有限公司咨询院研究中心
主任

朱敏，华信咨询设计研究院有限公司咨询院院长

张燕，华信咨询设计研究院有限公司咨询院副院长

如需获得有关华信咨询设计研究院有限公司咨询业务的详细资料，请发送邮件至：zhaoxuejian.hx@chinaccs.cn，电话联络：17826833663。

如需了解更多咨询业务的精彩洞察，请关注我们的官方微信账号：孜寻，ID: hx-Consulting，或“华信咨询设计研究院有限公司”。



关于华信咨询设计研究院有限公司

华信咨询设计研究院有限公司成立于 1984 年，总部位于浙江杭州，是中国通信服务的全资子公司。公司一直致力于通信、建筑、网信安全及行业信息化的研究咨询、设计与实施。作为国家级高新企业，综合实力位居全国同行前列，连续 8 年获住建部全国工程勘察设计企业勘察设计收入前 50。



华信拥有一支专注于数字基础设施及行业数字化建设运营全生命周期的规划咨询团队，为政府及企业客户提供精准的政策解读和行业洞察、科学的战略规划和决策支持、专业的投建采营维管理咨询、系统的数字化转型咨询、全面的组织队伍培训咨询和闭环的绩效评价服务。

深耕行业数十年，超 200 余人管理及数字化咨询顾问团队，已为国内外 24 个省份、200 余个城市的政府机构、事业部门、电信运营商及各行业企业，累计提供近万个战略决策、管理提升、数字化转型咨询解决方案，荣获国家及省部级奖励的咨询服务成果近百项。提供咨询与规划的方向有：

- 战略与市场咨询
- 组织和人力资源咨询
- 运营和 IT 咨询
- 供应链管理咨询
- 投资与绩效咨询
- 数字基础设施咨询
- 行业数字化咨询

我们的客户覆盖 100+国家₈和省部委、100+央国企、50+

行业领军企业，其中：

政府客户，主要包括国家省市区县各级政府，如大数据局、发改委、经信厅、政法委、交通厅、住建厅、教育厅、卫健委、医保局、文旅厅、自然资源厅、农业农村厅、市场监管局、园区管委会等。

企业客户，主要包括中国电信、中国移动、中国铁塔、中国广电、中国通信服务集团、中国人民银行、中国邮储银行、中交建集团、中国烟草集团、南方电网、国家电网、中国融通集团、中国商飞集团、阿里巴巴、华为、海康威视、大华股份、中兴通讯、烽火通信、中兵智航、杭钢集团、美利云集团、传化集团、杭州互联网交换中心、数字浙江、数字宁夏、山西云时代、安徽大众汽车、山东能源集团、四川煤炭产业集团、甘肃电投集团、河北高速集团、康恩贝集团、华数集团、浙江隧道、杭州数据交易所、杭州中房信息科技、杭州环境集团、安吉交投等。

科研机构，主要包括浙江大学、之江实验室等。



华信设计

华信咨询设计研究院有限公司

地址：浙江省杭州市滨江区春波路 999 号

网址：<http://www.hxdi.com>