2022
全球数字安全报告

－中国点亮数字时代的安全灯塔

CSA GCR cloud security alliance
GREATER CHINA REGION

联盟简介

云安全联盟(Cloud Security Alliance,CSA)是中立、权威的全球性非营利产业组织,于2009年正式成立,致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识,推动数字安全产业全面发展。

云安全联盟大中华区(Cloud Security Alliance Greater China Region, CSA GCR)作为CSA全球四大区之一,2016年在香港独立注册,于2021年在中国登记注册,是网络安全领域首家在中国境内注册备案的国际NGO,旨在立足中国,连接全球,推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

本白皮书由 CSA 大中华区专家撰写，感谢以下专家的贡献：

贡献者名单：

李雨航	姚凯	陈欣炜	方婷
高亚楠	顾伟	郭春梅	洪重良
姜宁	李博	林艺芳	刘洁
刘宇馨	刘玉红	鹿淑煜	马超
毛备	欧建军	苏泰泉	田原
王永霞	吴贺	肖达	杨天识
杨喜龙	余晓光	袁明坤	原浩
张光治	张淼	周杰	郭鹏程
黄连金	贾良钰	吕鹂啸	

贡献单位：

北京华云安信息技术有限公司　　北京启明星辰信息安全技术有限公司

北京数安行科技有限公司　　北京天融信网络安全技术有限公司

杭州安恒信息技术股份有限公司　　杭州美创科技有限公司

华为技术有限公司　　三未信安科技股份有限公司

腾讯云计算（北京）有限责任公司　　上海缔安科技股份有限公司

奇安信网神信息技术（北京）股份有限公司

（以上排名不分先后）

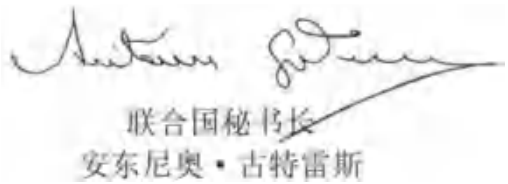
关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c-csa.cn/research） 上查看。

如本白皮书有不妥当之处，敬请读者联系 CSA GCR 秘书处给予雅正! 联系邮箱： research@c-csa.cn；国际云安全联盟 CSA 公众号。

引言

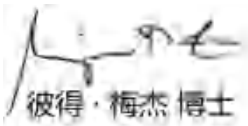
世界正以“比我们所能预测的更快的速度”从模拟技术向数字技术转变，这既带来了巨大希望，也带来了一些风险。新冠病毒大流行放大了数字世界的许多好处和危害。技术加强了医务人员的救生能力，允许企业远程操作等，同时技术也被严重滥用，仇恨言论、歧视和虐待正在数字空间蔓延。联合国“数字合作路线图”主要内容包括推动数字通用连接、促进数字技术成为公共产品、保证数字技术惠及所有人、支持数字能力建设、保障数字领域尊重人权、应对人工智能挑战、建立数字信任和安全。路线图的首要目标是“连接、尊重和保护数字时代的人们”。

有了正确的数字政策，数字技术才能前所未有地推动联合国可持续发展目标，特别是对于最贫穷的国家，但这需要更多的连接性和更少的数字碎片，更多跨越数字鸿沟的桥梁，和更少的障碍，普通人有更大的数字自主权，减少数字滥用和虚假信息。 很明显，如果没有指导和护栏，数字技术也有巨大的危害潜力——从压制言论自由到跨境恶意干扰，以及对在线人群（主要是女性）的攻击和骚扰。因此，我提出了一项全球数字契约，旨在为所有人创造一个开放、自由、包容和安全的数字未来，各国政府将在 2024 年联合国未来峰会上达成一致，并征求科技公司、民间社会、学术界和其他方面的意见。



序言

联合国秘书长发布的“数字合作路线图”是全球普惠数字技术发展数字经济的引航灯塔，随着数字化的不断发展，安全行业正在超越传统网络安全范畴，升级为数字安全。秘书长于 2021 年 9 月发布了《我们的共同议程》报告，提出将在联合国未来峰会上通过技术轨就全球数字契约达成一致。全球数字契约将成为“所有人共享开放、自由和安全的数字未来的共同原则”。国际云安全联盟大中华区对支持联合国秘书长的数字合作路线图与全球数字契约的落地起到了重要作用，本报告对“数字合作路线图”中的数字信任和安全提出了治理框架，并调研了全球各国的实施现状，报告发现中国在数字时代为数字经济提供的数字安全保障走在了全球前列。联合国科协与技术促进发展委员会与各成员国建议读者们吸取这些优秀实践，例如全球数字安全框架、新一代数据安全思考、中国神兽方阵报告、零信任理念、CAST 与 CNST 等，在全球范围共同建立数字信任和安全。在复杂的国际形势下，希望各方凝聚共识，推动合作，为经济复苏、携手应对全球挑战注入信心，联合国科技委期待中国为推动数字经济与数字科技的开放、包容、平衡、普惠发展贡献智慧和力量。



彼得·梅杰 博士
联合国科学技术发展委员会主席
联合国数字安全联盟名誉理事长

前言

随着数字经济、数字政府、数字社会等的快速发展，我们正处于数字时代。数字技术和数据不仅带来了新的理念、机遇和好处，也给所有国家带来了挑战、威胁和风险。消费者的数据安全和隐私保护已经从线下转移到线上，海量数据也引发了数个数据安全管理问题。随着数字技术为社会经济服务的范围和深度越来越大，安全问题的后果将更加严重。面对日益增加的安全风险，没有人可以单打独斗。数字安全不是单纯的技术问题，而是涉及业务、管理、流程、团队等多方面的系统工程。数字经济高质量发展涉及政策、法律、技术等多方面的协同配合。需要构建原生安全能力，以数字安全和可信为基础。

世界各国都在不断优化数据安全政策。欧盟发布的《欧洲数据保护监管局战略计划（2020-2024）》继续加强数据安全和个人隐私保护。美国发布《2020 年联邦数据战略和行动计划》，确立了保护数据完整性、确保流通数据真实性、数据存储安全等基本原则。《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》也于 2021 年颁布。本文档基于 CSA 大中华区提出的数字安全 REE 框架，调研了全球数字安全各领域的现状，并总结了优秀的实践、流行的技术，和公认的数字安全提供商，还包括全球重要的法律、法规、标准，向读者介绍数字安全的发展概况，特别是中国的状况。希望该文件能成为政府与行业在数字安全方面的参考，帮助人们构建更加安全的数字环境。

李雨航 院士，Yale Li

CSA 大中华区主席兼研究院院长

目录

第一章 数字时代的到来

1.1 第四次工业革命

制造业作为国家的基础设施和立国之根本，从来都是一个国家立足世界的重要筹码。人类历史经历了几个大的工业革命，从蒸汽技术革命、电力技术革命、计算机及信息技术革命，直到今天的第四次工业革命。

在国际上影响比较大的与第四次工业革命有关几个事件包括：

- 美国早在 2012 年 2 月就发布了《先进制造业国家战略计划》，踏上了新一轮工业革命的道路，美国电报电话公司、思科、IBM 等还组建了工业互联网联盟（IIC）。
- 德国工业 4.0。2013 年，在莱纳河畔汉诺威工业博览会如期举办。在这场全球工业界的盛会上，主办方德国正式提出了“工业 4.0”战略。按照德国当时的定义，“工业 4.0”是指利用物联信息系统将生产中的供应、制造、销售信息数据化、智慧化，最后达到快速、有效、个人化的产品供应。通过产业数字化，人类的生产效率得到了极大的提高。互联网可以把全球的消费者市场连接到一起，而供应链数字化更是极大提升了生产的效率及单位生产成本，从而赢得更大的市场。
- 日本这位工业 3.0 时代的优等生，推出了《日本再兴战略》，将工业 4.0 视为创造新商业模式的重要契机，重点发展物联网、人工智能和大数据技术。日本希望追上工业 4.0 的快车，再现“日本制造”的荣光。
- 作为世界第二大经济体的中国，在 2015 年 5 月推出中国版工业 4.0 纲领性政策文件——《中国制造 2025》，主动应对新一轮科技革命和产业变革的重大战略选择。

美国、德国、日本和中国这几个国家的工业在世界上占有举足轻重的地位。这些国家都在积极布局，并且采取相应的行动。更多的国家同样在推进第四次工业革命的落地。目前，大部分人认为工业 4.0 可以等同于第四次工业革命。

工业 4.0 的本质，就是通过数据流动自动化技术，从规模经济转向范围经济，以同质化规模化的成本，构建出异质化定制化的产业。对于产业结构改革，这种转变至关重要。大家对工业 4.0 的定义存在差异，德国叫工业 4.0，美国叫工业互联网等等，但大体内容还是保持一致的。第四次工业革命涌现了物联网、人工智能、大数据、区块链等

技术。这些技术的出现将人类的生态带入了另外一个高度。

第四次工业革命正在如火如荼的推进，各个国家都不想在这场革命浪潮中落伍。谁在第四次工业革命浪潮中占领优势，就有可能改变世界格局。目前，全世界都在思考一个问题：第四次工业革命的核心突破点在哪里？

1.2 数字经济

目前普遍认为数字经济是第四次工业革命的突破点。数字经济的定义比较宽泛，目前得到广泛认可的是《G20 数字经济发展与合作倡议》中给出的定义：

数字经济，是指以使用数字化的知识和信息作为关键生产要素、以现代信息网络作为重要载体、以信息通信技术的有效使用作为效率提升和经济结构优化的重要推动力的一系列经济活动。

随着云计算、大数据、人工智能等新一代信息技术的不断突破和广泛应用，一个迹象已经显现：数字经济，正在成为全球经济增长的新动能。

联合国发布的《数字经济报告 2021》证实了数字经济正在非常快速的发展。

2022 年包括国内和国际流量在内的全球互联网流量将超过截止 2016 年的互联网流量之和。新冠疫情导致越来越多的活动在网上进行，对互联网流量带来巨大影响。2020 年全球互联网带宽提高了 35%，是 2013 年以来增幅最大的一年。据估计，大约 80%的互联网流量与视频、社交网络和游戏有关。每月的全球数据流量预计将从 2020 年的 230EB 激增到 2026 年的 780EB。从参与数据驱动的数字经济并从中受益的能力来看，美国和中国脱颖而出。全世界的超大规模数据中心有一半位于这两个国家，这两个国家的 5G 普及率最高，人工智能初创企业融资总额占过去五年的 94%，研发人员占世界顶尖人工智能研究人员的 70%，数字平台市值占全球最大数字平台市值总和的近 90%。纽约证券交易所综合指数在 2019 年 10 月至 2021 年 1 月期间增长了 17%，但顶尖数字平台的股票价格的涨幅却从 55%（Facebook）到 144%（苹果）不等。

早在 2019 年，中国信息通信研究院发布的《全球数字经济新图景》就显示，2018 年，47 个国家的数字经济总规模超过 30.2 万亿美元，占 GDP 之比高达 40.3%。其中，有 38 个国家数字经济增速显著高于同期 GDP 增速。

回顾美国的数字经济历程可以追溯到上个世纪的“信息高速公路”。

- 信息高速公路

上世纪 90 年代，克林顿政府高度重视并大力推动信息基础设施建设和数字技术发

展，引领世界进入数字时代。这种推动与副总统戈尔有着莫大关系。戈尔在全球率先提出了著名的“信息高速公路”和“数字地球”概念。

上世纪 80 年代初期，戈尔在担任众议员期间，就呼吁建立一个全国性的“信息高速公路”。戈尔当选副总统后，一直是克林顿政府建设国家信息高速公路的核心人物。

1993 年 9 月，美国政府公布“国家信息基础设施行动计划”，信息高速公路战略开始落地。该文件开宗明义地指出：“国家信息基础设施的发展能够帮助引发一场信息革命，这场革命将永远改变人们的生活、工作和交流方式。”

上世纪 50 年代州际公路系统的建设，为美国半个世纪的繁荣奠定了坚实的基础。四十年后的信息高速公路可与之媲美，甚至更加伟大，为美国数字经济插上了腾飞的翅膀。

- 美国商务部构建完备的政策体系

自 1998 年到 2018 年的 20 年间，美国商务部就数字经济和数字国家发布了 13 份重磅报告，探讨数字经济发展的前沿和热点问题。这些报告如下表所示。

序号	时间	名称
1	1998 年	浮现中的数字经济
2	1999 年	浮现中的数字经济（二）
3	2000 年	数字经济 2000
4	2002 年	数字经济 2002
5	2003 年	数字经济 2003
6	2010 年	数字国家：21 世纪美国通用互联网宽带接入进展
7	2010 年	探索数字国家：美国家庭宽带互联网应用
8	2011 年	数字国家：扩大互联网使用
9	2011 年	探索数字国家：计算机和互联网家庭应用
10	2013 年	探索数字国家：美国新兴在线体验
11	2014 年	探索数字国家：拥抱移动互联网
12	2016 年	在数字经济中实现增长与创新
13	2018 年	数字经济的定义和衡量

表 1-1 美国政府 1998 到 2018 年间与数字经济有关的报告

不仅仅是美国，世界上其他国家也在加速数字经济的布局。

欧盟于 2021 年 3 月发布了《2030 数字化指南：实现数字十年的欧洲路径》纲要文件，涵盖了欧盟到 2030 年实现数字化转型的愿景、目标和路径。日本自 2013 年开始，每年制定科学技术创新综合战略，从“智能化、系统化、全球化”视角推动科技创新。俄罗斯 2017 年将数字经济列入《俄联邦 2018—2025 年主要战略发展方向目录》，并编制完成俄联邦数字经济规划。中国于 2015 年党的十八届五中全会将大数据上升为国家战

略，之后出台了 10 余项促进数字经济行业发展的政策，2017 年起连续 5 年将数字经济相关内容写入政府工作报告。

数字经济一般可以分为两部分：

- 数字产业化。主要是指信息通信产业（ICT），主要包括电子信息制造业、电信业、软件和信息技术服务业、互联网行业等。
- 产业数字化。主要指传统产业由于应用数字技术所带来的生产数量和生产效率提升，例如工业互联网、智能制造、平台经济等融合型新产业。

无论是数字产业化还是产业数字化，核心都是数字。数字贯穿着全部过程。通常，我们也可以把数字化的信息和知识描述成数据。数字经济建立在数据的基础之上，中国已经把数据列为基本生产要素，和土地、资本、人才、科技一样。作为第五大基本生产要素，数据的价值正在体现，从而推动着数字经济往前走。

人类已经处于数字时代的潮流中，数字经济、数字政府、数字军事、数字社会、数字文明等都在加速推进中。近年来比较火热的虚拟世界、元宇宙也是数字时代的产物。数字经济作为一种新的经济形态，比重正在逐年增加；数字政府让民众可以随时随地利用任何设备获取政府信息和服务；数字社会让整个社会的运转基于数字；元宇宙更是建立了一个新的数字世界。

全球数字经济发展迅猛。据中国信息通信研究院数据，2020 年，发达国家数字经济规模达到 24.4 万亿美元，占全球总量的 74.7%。发达国家数字经济占国内生产总值比重达 54.3%，远超发展中国家 27.6%的水平。从增速看，发展中国家数字经济同比名义增长 3.1%，略高于发达国家数字经济 3.0%的增速。2020 年，全球 47 个国家数字经济增加值规模达到 32.6 万亿美元，同比名义增长 3.0%，产业数字化仍然是数字经济发展的主引擎，占数字经济比重为 84.4%。从规模看，美国数字经济继续蝉联世界第一，2020 年规模接近 13.6 万亿美元。从占比看，德国、英国、美国数字经济在国民经济中占据主导地位，占国内生产总值比重超过 60%。从增速看，中国数字经济同比增长 9.6%，位居全球第一。2022 年中国信息通信研究院发布了《中国数字经济发展报告（2022 年）》，指出 2021 年中国数字经济的规模达到了 6.9 万亿美元，占 GDP 的比重达到了 39.8%。数字经济年均增速高达 15.9%，显著高于同期 GDP 的平均增速，数字经济已经成为支撑经济高质量发展的关键力量。

可以预期，数字经济在未来较长一段时间都将保持快速增长。

1.3 数字政府

数字政府是综合运用互联网、物联网、大数据、人工智能、区块链等现代信息技术，为促进经济社会运行全面数字化而建立的一种新型政府形态。

随着互联网、大数据、区块链等现代信息技术的不断普及，越来越多的国家积极利用信息技术创新政府运作方式、推动数字政府建设。2020 年全球新冠肺炎疫情暴发，进一步推动了数字技术在政府信息公开、便民服务、动态监管、智能决策等方面的运用。根据最新发布的《2020 年联合国电子政务调查报告》，全球电子政务发展平均指数(EGDI)从 2018 年的 0.55 上升到 2020 年的 0.60，EGDI 指数处于“高”或“非常高”级别的成员国共有 126 个，占所有成员国的 65%。由全球 EGDI 指数持续上升可看出，世界大多数国家积极推动数字政府建设，重视整合线上和线下渠道，以实现政府数字治理能力的现代化。

2020 年 2 月，中国深化改革委员会第十二次会议指出要运用大数据、人工智能、云计算等数字技术，在疫情监测分析、病毒溯源、防控救治、资源调配等方面更好发挥支撑作用。同年 10 月，中国的十九届五中全会审议通过的《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》提出加强数字社会、数字政府建设，提升公共服务、社会治理等数字化智能化水平。数字政府是数字中国体系的有机组成部分，是推动数字中国建设、推动社会经济高质量发展、再创营商环境新优势的重要抓手和主力引擎。

中国的数字政府成熟度在世界上的排名并不高，更多发达国家的数字政府起步更早。起步最早的当属美国。美国从上个世纪 90 年代开始就部署数字政府，近年来，美国先后发布《数字政府服务》《数字政府：构建一个 21 世纪平台以更好地服务美国人民》等战略规划，致力于提供可以在任何时间、任何地点、通过任何设备获取的数字政府服务。

新加坡先后发布《智慧国家 2015》和《智慧国家 2025》，秉持“大数据治国”的理念，致力于实现“多个部门、一个政府”目标，为公众提供优质便捷的公共服务。丹麦制定《2016—2020 年数字战略》，加强数字公共管理与电子服务建设，同时强调政府与企业及其他利益相关组织团体的合作。韩国发布《2020 年电子政务总体规划》，内容包括提供数字化的政府服务、创建数字友好型产业、建立电子政务平台等具体措施。

纵观世界各国，数字政府热潮正在快速推进中。数字政府建设注重实现政府决策智能化、权力运行透明化、公共服务精准化、绩效评估科学化、流程再造高效化等目标，

努力打造“政府即平台”。

除了数字经济、数字政府之外，数字文化、数字社会、数字军事等其他各行各业的数字化也正处于快速的发展之中。

1.4 数字时代的意义

可以毫不夸张的讲，任何行业、任何地方、任何领域都离不开数字。不管是无人驾驶，还是新材料，生物技术，核聚变等等，都必须基于新型的数字化工具、数字化技术，和人工智能。数字时代对于人类的意义是非常巨大的，下面只是几个示例：

- 消费者仅仅需要一部手机，就能学习、生活、工作；
- 企业通过数字，打通各个环节，减少成本、创造增量，提高企业的效率和利益。
- 政府通过数字化转型，打通多部门之间的协作，提高办事效率。
- 监管机构通过数字，掌控各行各业的具体信息，引导行业正确、健康地发展。
- 医院通过数字展示病人的病情，通过对数字的分析，为病人提供最优的医疗方案。

人类所处的数字时代将会持续很长一段时间，为了进一步推动数字时代前进，我们还有很多事情要做，比如：

- 完善公共数据开放共享机制。建立健全高效的公共数据共享协调机制，支持打造公共数据基础支撑平台，推进公共数据归集整合、有序流通和共享。
- 建立健全数据流通交易规则。探索“原始数据不出域、数据可用不可见”的交易范式，在保护个人隐私和确保数据安全的前提下，分级分类、分步有序推动部分领域数据流通应用。
- 拓展规范化数据开发利用场景。发挥领军企业和行业组织作用，推动人工智能、区块链、车联网、物联网等领域数据采集标准化。
- 加强数据安全保护。强化网络安全等级保护要求，推动完善数据分级分类安全保护制度，运用技术手段构建数据安全风险防控体系，使数据始终处于控密双态计算，实现“动静用转”和“云网边端”全面覆盖，探索完善个人信息授权使用制度。

数字时代建立在数字基础之上，围绕着数字建立了一个庞大的数字生态。这是一个非常复杂而且长期的工程，我们所面临的挑战也非常巨大。然而数字时代的到来是不可阻挡的，我们需要做好各项工作，迎接这一转变，让数字发挥更大的作用。数字时代是一个伟大的时代，必将会在人类历史上留下重重的一笔。让我们拥抱数字时代的到来吧。

第二章 数字安全框架

数据要素在市场化流通的过程中，需要安全、可信、和隐私的保障，数字经济的发展离不开健全的数字经济治理体系和可靠的数字经济安全体系。

数据作为生产要素对数据安全带来全新的挑战，提出了更高要求，数据安全与信息安全、网络安全并列，构成了数字安全的重要部分。新一代数据安全遵循“原生安全 Meta Security”的核心理念，秉承“天然一体、主动免疫、始终验证、持续防护”的原则，具有“原生一体、安全可信”，覆盖“动静用转”和“云网边端”，真正实现数字可信与安全。特别是数据流动的全球化、地域属性的合法合规监管要求，传统的“动静用安全”的外挂堆砌式被动防范数据安全带来巨大挑战，其碎片化、系统性不足、被动安全机制，无法应对今天和未来的威胁攻击，特别是使用和流转中的风险威胁。新一代数据安全的原生性体现在“原生安全”的理念，天然防护抗体与存储计算通讯形成原生一体安全可信防护体系，具备“天然一体、主动免疫、始终验证、持续防护”，不仅安全而且可信；在存储计算通讯的同时并行实时进行安全可信防护，逐级验证构建可信链条，提供存储计算通讯的安全可信，确保的数据资源和操作全程可测可控，提供安全可信的存储计算通讯环境“主动免疫”；宿主和抗体成为原生一体，让安全与资源“同体共生”，管控“如影随行”；数据与其权利、权益和权限“天然一体”、“密不可分”，实现数据的“密不透风”；保障数据在“动静用转”等状态的安全可信，被动防御与主动保护相融合，实现“动态防御、主动保护、纵深防控、立体防护、主动免疫、安全可信”，使数据始终处于控密双态计算（Control & Crypto Computing），实现“动静用转”和“云网边端”全面覆盖，在保障数据相关各方权益的同时，打通数据孤岛共享共赢，做到合规可监管，支持多次交易，发挥各大数据平台和交易所的作用，有效防范供应链、合作伙伴、外贼、离在职人员、流氓勒索等各种风险威胁，做到数据可信与安全；充分发挥数据作为生产要素的重要价值和意义，为数字经济保驾护航。

数字安全的发展和数字时代的发展一脉相承。新技术带来新挑战，新挑战需要新思维，新思维创造新机会。数据作为至关重要的生产要素，需充分发挥数据作为生产要素的重要价值和意义，数据安全必须放在首要位置，新一代数据安全的落地亟需数据安全法律、治理、技术多维并举。为了助力数字经济安全发展，国际云安全联盟大中华区联合各界安全精英经过一年的精心打磨，于 2022 年 3 月 11 日正式发布数字安全框架。该框架涵盖了数字安全的定义、REE(Regulation, Execution， Evaluation)数字安全框架、数字身份框架和原生安全框架。

2.1 数字安全的定义

数字安全是指在数字时代与数字化相关的一切安全要素、行为和状态的集合，既包括保障数字经济的安全性，也包括将数字技术用于安全领域。数字安全以数字身份为核心，以原生安全为基础底座，涵盖了信息安全、网络安全、数据安全、隐私保护等领域或场景，并可扩展（如元宇宙安全）。除此之外，数字安全还包括利用数字技术保障数字基础设施的物理安全。虽然数字安全更偏重数字经济与数字技术，但是与偏重国家网络主权的网络空间安全(Cybersecurity)在法律、标准、技术上也是相通的。数字安全的定义如图 2-1 所示：

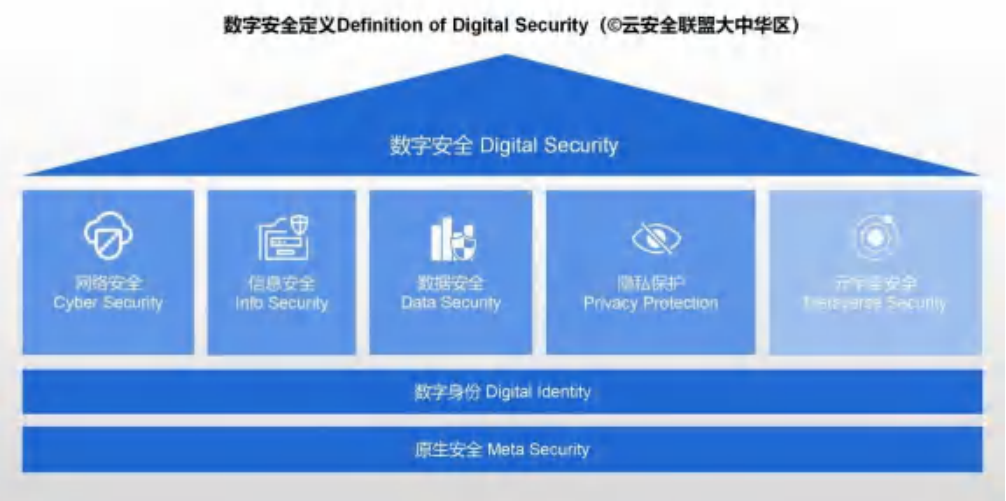


图 2-1 数字安全的定义

2.2 数字安全的内涵

数字安全涉及网络安全、信息安全、数据安全、隐私保护、以及新兴的元宇宙安全，同时涵盖数字身份和原生安全，各领域的具体含义如下：

- **网络安全 (Cyber Security)**: 保障网络系统的软硬件安全，负责人是 CSO、CISO、CTO、CIO 等。
- **信息安全** (Information Security): 保障一切有价值信息的安全，负责人是 CISO、CIO 等。
- **数据安全** (Data Security): 保障数据全生命周期的安全与合规，负责人是 CDO、CIO、CISO、CSO 等。
- **隐私保护** (Privacy Protection): 保护用户的隐私与个人信息，负责人是 CPO、

DPO 等。

- **元宇宙安全**（Metaverse Security）：保障通过数字化形态承载的虚实相生、虚实相融的平行宇宙的安全，这是未来数字安全的主要扩展领域。
- **数字身份** (Digital Identity)：作为连接安全与业务的基座，提供对所有的人、数字人、物、设备等的数字标识、认证、访问的全生命周期管理。
- **原生安全** (Meta Security): 原生安全是下一代互联网原生安全，包括云计算、大数据、AI、5G/6G、IoT、区块链、量子计算等新兴技术所涉及的系统的原生安全，它是数字安全的底座，需要硬件信任根的支持。

2.3 REE 数字安全框架

REE(Regulation, Execution， Evaluation)数字安全框架是国际云安全联盟大中华区于 2022 年 3 月 11 日正式发布的数字安全的定义 (Definition of Digital Security) 的重要组成部分。共分为规则层（数字安全框架的战略指引）、执行层（规则层落地所需的一切资源/工具及使用这些资源/工具的具体行动）和评价层（针对组织的数字安全成熟度进行评估、验证及考核）三层。

REE 详情如图 2-2 所示：

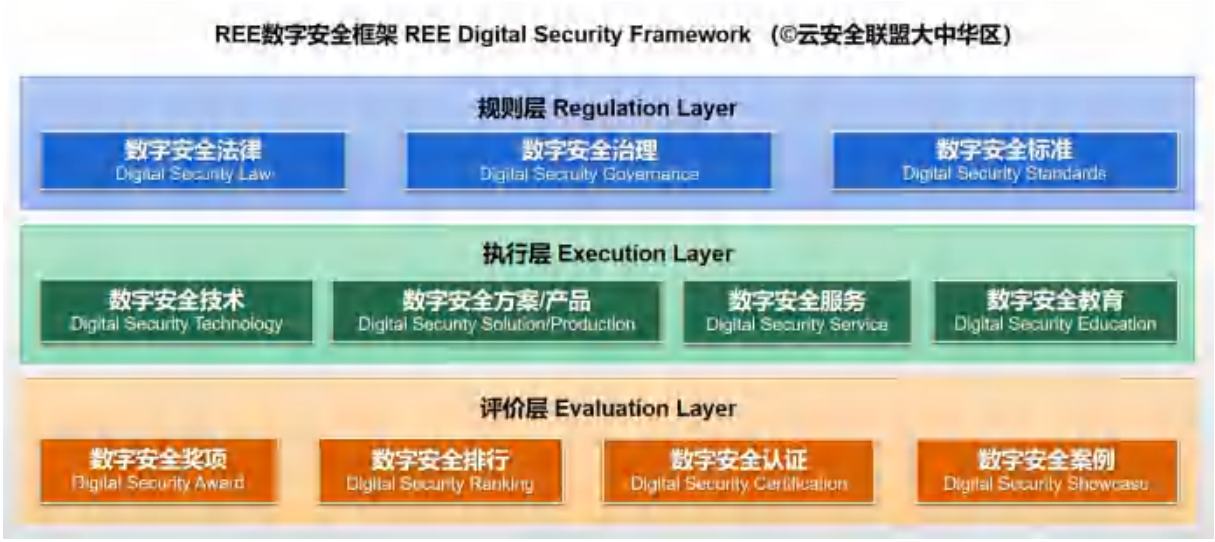


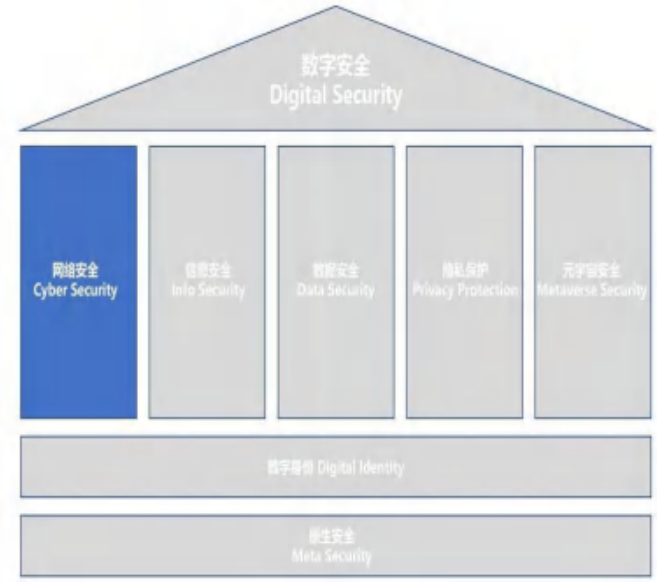
图 2-2 REE 数字安全框架

- **规则层**（**Regulation** Layer）：规则层是数字安全框架的战略指引，主要包含数字安全法律、数字安全治理、数字安全标准等内容。这一层需要解决数字安全法律、法规、规章、政策、监管、标准等问题，为组织的数字安全建设与合规治理提供策略指导。

- **执行层**（Execution Layer）执行层涵盖了规则层落地所需的一切资源/工具及使用这些资源/工具的具体行动，主要包括数字安全技术、数字安全方案/产品、数字安全服务、数字安全教育等内容。这一层需要解决数字安全技术的研究与进步、数字安全方案/产品的研发与应用、数字安全服务的开展（如安全咨询、安全运营等）、数字安全人才的培育等方面的问题，是组织实现数字安全目标的核心。
- **评价层**（Evaluation Layer）：评价层针对组织的数字安全成熟度进行评估、验证及考核，主要包含数字安全奖项、数字安全排行、数字安全认证、数字安全案例等内容。这一层需要通过安全认证/审计/测评等方式对组织的数字安全能力进行持续评估，从而促进持续改进和提升，实现从规则、执行、评价到改进的安全闭环。除此以外通过数字安全奖项、数字安全排行榜/象限及数字安全优秀案例分享的方式进行相关的市场宣传和引导，从而促进数字安全产业的发展。

2.4 网络安全

网络安全是保障网络系统的软硬件安全，涉及的框架主要有：



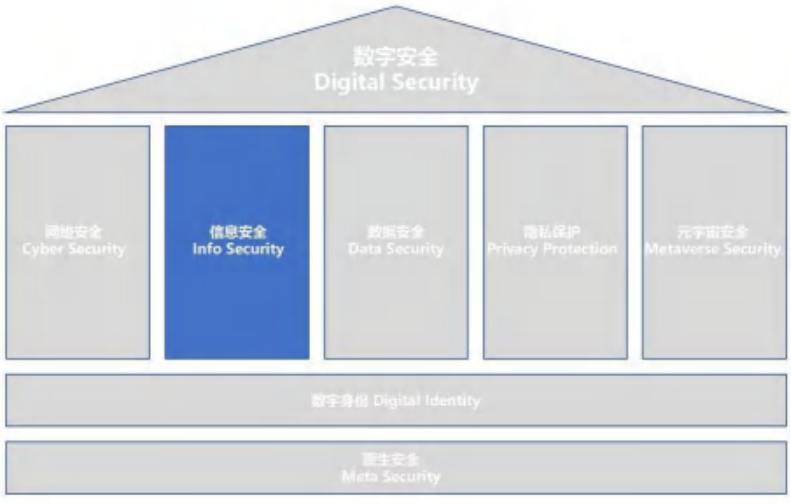
2.4.1. NIST-CSF 框架

CSF（Cybersecurity Framework）由 NIST 与私营和公共部门密切合作开发，是美国各组织自愿采用的基于风险的方法。这个自愿性框架最初是为了应对国家关键基础设施（CI）领域的网络安全挑战而开发的，世界各地各类组织随后对该框架的广泛使用证明了该框架的普遍适用性。CSF 核心的五项功能是识别、保护、检测、响应、恢复（Identify, Protect, Detect, Respond, Recover）。这五项功能提供了一个高层级的风险管理词汇，既对网络安全专家有意义，也方便非网络安全专家使用。因此，这些功能既适用于网络安全风险管理，也适用于企业风险管理。

2.4.2. MITRE ATT&CK®框架

MITRE 在 2013 年推出了 ATT&CK 模型，根据真实的观察数据描述和分类对抗行为。ATT&CK 将已知攻击者行为转换为结构化列表，将这些已知的行为汇总成战术和技术，并通过几个矩阵以及结构化威胁信息表达式（STIX）、指标信息的可信自动化交换（TAXII）表示。由于此列表相当全面地呈现了攻击者在攻击网络时所采用的行为，因此对于各种进攻性和防御性度量、表示和其他机制都非常有用。ATT&CK 会详细介绍每一种技术的利用方式，以及为什么了解这项技术对于防御者很重要。ATT&CK 模型极大地帮助了安全人员更快速地了解不熟悉的技术。

2.5 信息安全



信息安全是从体系上保障一切有价值信息的安全，涉及的框架主要有：

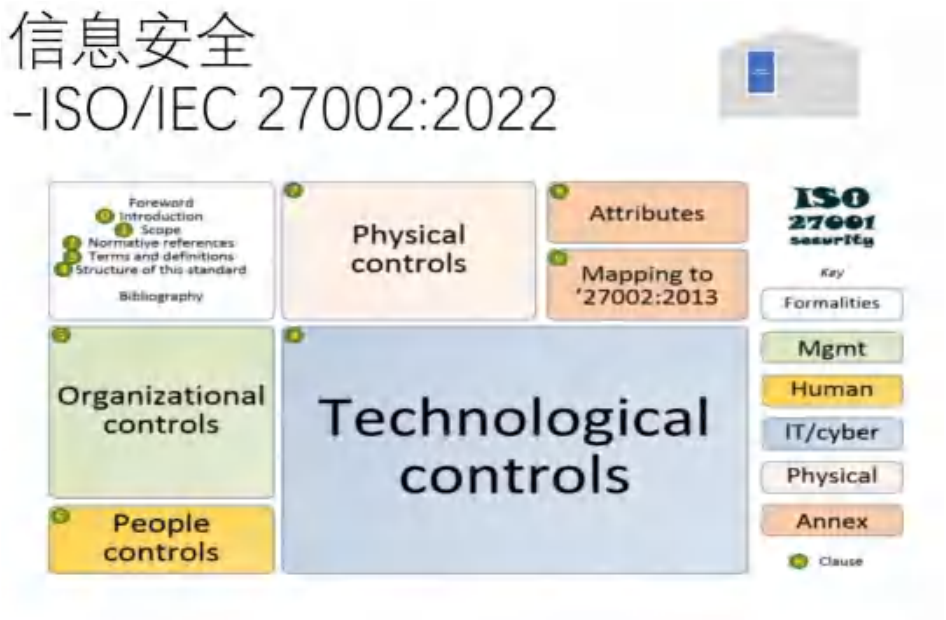
2.5.1. ISO27001 框架

国际标准化组织（ISO）是一个独立的非政府组织，也是世界上最大的自愿国际标准制定者。国际电工委员会（IEC）是制定和出版电气、电子及相关技术国际标准的世界领先组织。

ISO/IEC 27000 系列标准由 ISO/IEC 联合小组委员会发布，概述了数百种控制措施和控制机制，帮助各种类型和规模的组织保持信息资产的安全性。这些全球标准为政策和程序提供了一个框架，包括组织信息风险管理过程中涉及的所有法律、物理和技术控制措施。

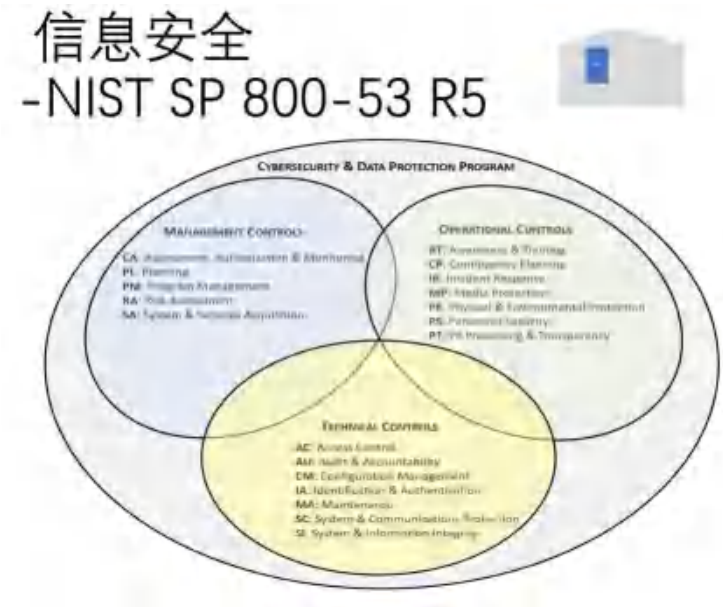
ISO/IEC 27001 是一项安全标准，正式规定了信息安全管理系统（ISMS），旨在将信息安全置于明确的管理控制之下。作为正式规范，该标准要求定义如何实施、监控、维护和持续改进 ISMS 的需求，还规定了一组最佳实践，包括文档要求、责任划分、可用性、访问控制、安全性、审计以及纠正和预防措施。ISO/IEC 27001 认证有助于组织遵守与信息安全相关的众多法规和法律要求。

2.5.2. ISO/IEC 27002:2022 框架



2022 年 2 月，ISO(国际标准化组织)更新发布了《ISO/IEC 27002:2022 信息安全、网络安全和隐私保护-信息安全控制》，作为组织根据信息安全管理体系认证标准定制和实施信息安全控制措施的指南。2022 版将控制措施分配到组织、人员、物理、技术的四个大主题，使分类更加简单，方便组织对安全控制点进行选择归类，可以通过归类的特定主题策略支持信息安全策略，加强信息安全控制的实施。

2.5.3 NIST SP 800-53 R5 框架



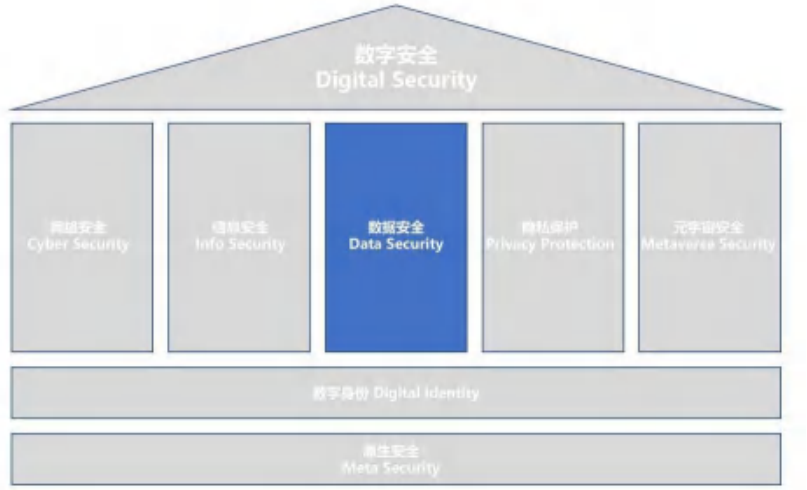
SP 800-53 一直视作是 NIST 信息安全的支撑性文件，最新的更新，直接产生了第一

个全面的安全和隐私控制目录。NIST SP 800-53 版本 5 不是一个小的更新，而是一个完整的更新，解决了结构问题和技术内容。这项更新是多年的努力，旨在开发第一个全面的安全和隐私控制目录，可用于管理任何部门和规模的组织的风险，以及从超级计算机到工业控制系统再到物联网（IoT）设备的所有类型系统的风险。这些控制措施提供了一种积极主动和系统性的方法，确保关键的系统、组件和服务具有足够的可信度，并具有必要的恢复力，可以维护经济利益和国家安全。

2.5.4 CIS Critical Security Controls V8 框架

CIS 关键安全控制是一组优先保护措施，用于防范和缓解针对系统和网络的普遍攻击。CIS 的前身也被称作 SANS。CIS Controls 框架列出了 18 个控制域，每个域都很多详细的控制要求。非常适合企业参照具体的控制项开展工作。CIS Controls v8 已经发布，更新了对云计算、虚拟化、移动化、外包、居家办公的支持，有效的防范不断变化的攻击方式，并在企业迁移到云和混合环境时提供安全性保护。

2.6 数据安全



数据安全保障数据全生命周期的安全与合规，涉及的框架主要有：

2.6.1 GB/T 37988—2019 框架

《GB/T 37988—2019 数据安全能力成熟度模型》给出了组织数据安全能力的成熟度模型架构，规定了数据采集安全、数据传输安全、数据存 储安全、数据处理安全、数据交换安全、数据销毁安全、通用安全的成熟度等级要求。本标准适用于对组织数据安全能力进行评估，也可作为组织开展数据安全能力建设时的依据。

数据安全能力成熟度模型（DSMM）

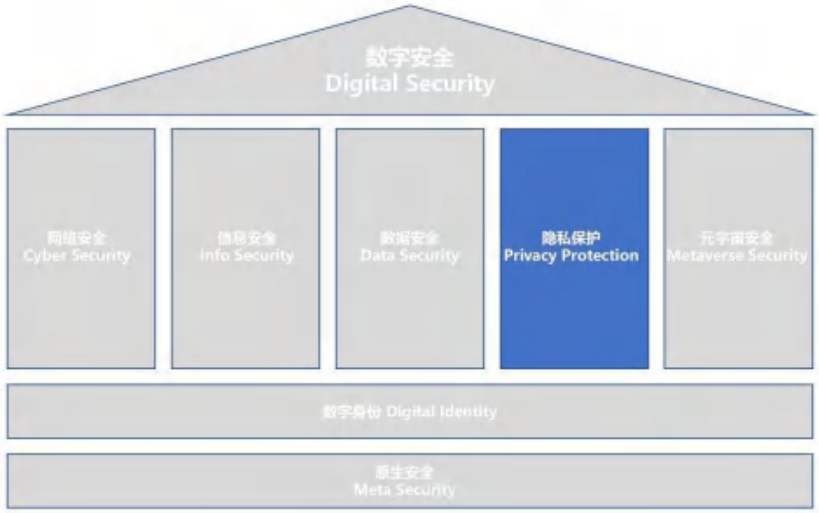
DSMM 架构主要由安全能力、能力成熟度等级，以及数据安全过程三个维度构建而成。

在安全能力维度，明确了组织在数据安全领域应具备的能力，包括组织建设、制度

流程、技术工具和人员能力。

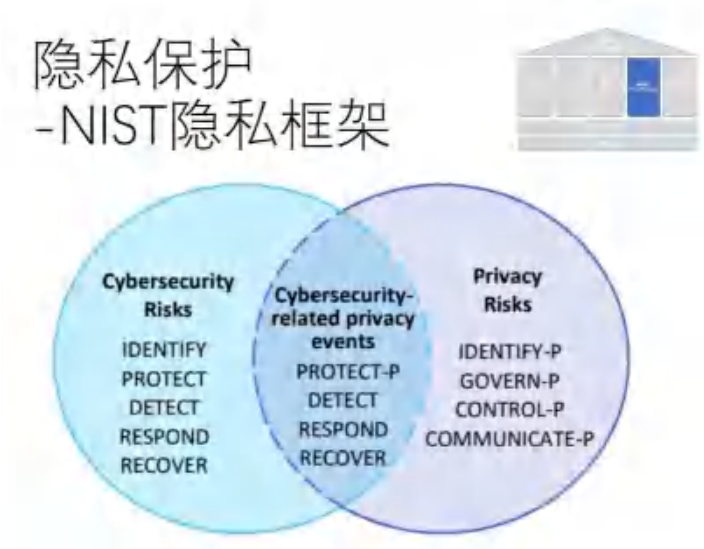
在能力成熟度等级维度将等级划分为五级,具体而言：1 级是非正式执行级，2 级是计划跟踪级，3 级是充分定义级，4 级是量化控制级，5 级是持续优化级。数据安全过程维度定义了数据安全过程，其中包括数据生存周期安全过程和通用安全过程。数据生存周期安全过程具体包括数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全和数据销毁安全 6 个阶段。

2.7 隐私保护



隐私保护保护用户的隐私与个人信息，涉及的框架主要有：

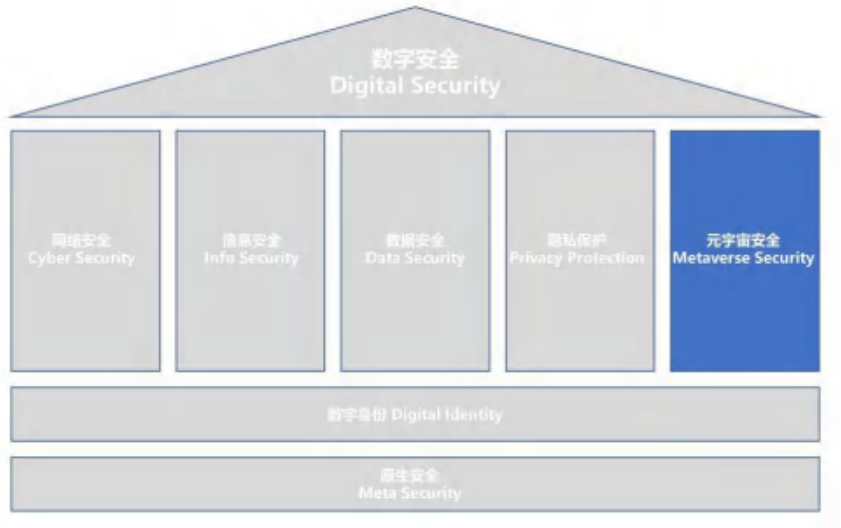
2.7.1 NIST 隐私框架



NIST 隐私框架是一种通过企业风险管理（隐私框架）改善隐私的工具，旨在广泛适

用于各种规模的组织，以及各种特定的技术、行业、法律或管辖权。隐私框架使用一种适用于任何组织在数据处理生态系统中的角色的通用方法，目的是帮助组织管理隐私风险

2.8 元宇宙安全



元宇宙可以定义为人们连接、互动和购物的虚拟环境。维基百科将元宇宙定义为“互联网的假设迭代，它是一个单一的、普遍的、身临其境的虚拟世界，通过使用虚拟现实和增强现实眼镜促进。 在通俗的使用中，元宇宙是一个专注于社交联系的 3D 虚拟世界网络。”

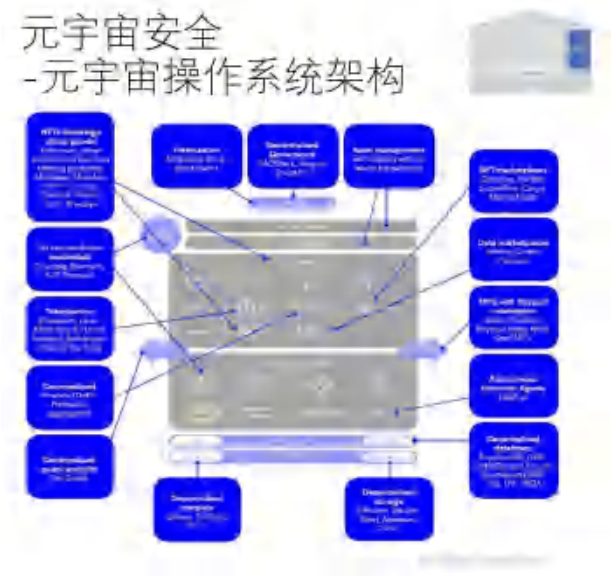
元宇宙有两种主要形式：

1. 虚拟现实通过 VR 眼镜提供人工现实。 它接管了用户的视野以提供身临其境的体验。其他形式的沉浸式体验包括身体的音频和位置跟踪，以使身体部位（例如手）的运动能够与虚拟环境进行交互。

2. 增强现实 (AR) 的沉浸感不如 VR。它通过某种类型的镜头在现实世界之上添加虚拟叠加层。用户仍然可以正常查看周围环境。主机可以看到用户的位置并且可以猜测他们的意图。 对 AR 的隐私期望高于 VR。

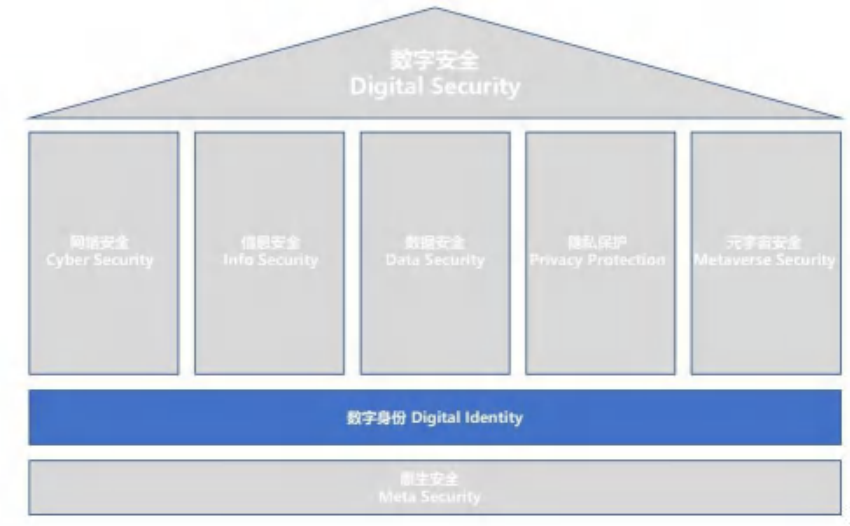
元宇宙安全保障通过数字化形态承载的平行宇宙的安全，是未来数字安全的主要扩展领域。

2.8.1 元宇宙操作系统框架



目前，OpenMetaverse 操作系统主要集中在关键的底层，包括在世界经济中不可协商的功能，如用户主权身份和资产，以及与经济之间的桥梁，以及彼此之间的复杂游戏引擎、3D 建模工具链，以及主要集中的世界的呈现堆栈。针对该框架中的每个子域，都需要采取合适的安全控制措施。

2.9 数字身份



数字身份是连接安全与业务的基座，提供对所有的人、数字人、物、设备等的数字标识、认证、访问的全生命周期管理，数字身份涉及的框架有：

2.9.1 数字身份框架 Digital Identity Framework

身份定义安全联盟（IDSA）的创建是为了帮助企业认识到将身份和安全结合起来的重要性，通过以身份为中心的安全策略减少漏洞的风险。IDSA 更重要的目的是将问题分解为以身份为中心的安全成果和实施方法，为从业者提供指导和提示。

数字身份是连接安全与业务的基座，当元宇宙兴起之时，数字身份更是连接现实世界和虚拟世界的标识和桥梁。图 2-3 是身份定义安全联盟（IDSA）的示意图，描述了身份验证如何工作，其中人机用户都是该过程的一部分。

图 2-3 数字身份框架

数字身份框架以四个基本概念为基础。

- 身份识别是一项关键的网络安全技术
- 网络安全的所有方面必须从根本上协同工作，才能取得有意义的效果
- 每个商业交易、攻击面或目标都涉及到一个证书和一个服务或数据。
- 考虑到在安全方面的累积，每一项新投资都使得整体安全能力变得更加有效。

身份定义安全框架由领先的供应商、解决方案提供商和从业人员合作开发，为企业提供了实施以身份为中心的安全方法的实用指导。身份定义安全框架为从业人员提供了

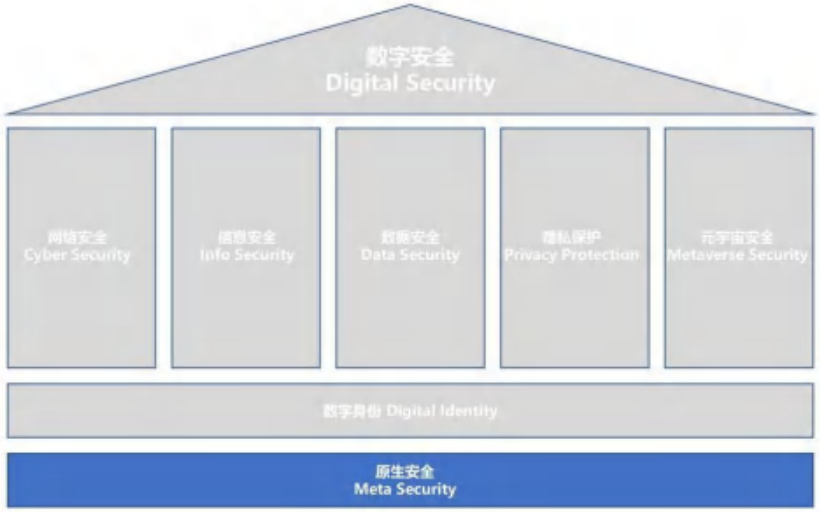
一套基本的构件以及蓝图和最佳实践，有助于实现支持业务需求的安全成果。

身份定义的安全结果是一种期望的结果，通过以身份为中心的安全改善组织的安全态势并降低安全风险。以身份为中心的安全减少了漏洞或审计失败的风险。

身份定义安全成果可以通过许多不同的身份定义安全实施方法实现。这些方法定义明确的模式，结合了身份和安全能力，帮助组织利用身份背景改善安全态势。

以身份为中心的安全方法的基础最好是以成熟的身份和访问管理（IAM）开始。IDSA 最初定义的一套最佳实践侧重于 IAM 的基本原理，作为与 IAM 项目的人员和流程以及技术方面有关的推荐，并作为 IAM 项目的补充，增强以身份为中心的安全方法的基础。

2.10 原生安全



2.10.1 原生安全框架 Meta Security Framework

原生安全是指下一代互联网原生安全，包括云计算、大数据、AI、5G/6G、IoT、区块链、量子计算等新兴技术所涉及的系统的原生安全，是数字安全的地基，需要硬件信任根的支持。原生安全的特点包括安全与产品融合，具有硬件可信根，零代理不需安装，匹配可信计算环境，核心软件可形式化验证，主动检测动态防御（防勒索能力，防病毒能力，防 APT 能力，防 DDOS 能力等），可信启动与安全度量等特点。原生安全框架如图 4 所示：

图 2-4 原生安全框架

- **无处不在的可信 AI：**通过可信 AI 实现安全监控、入侵检测、态势感知、恶意代码检测、代码审计、漏洞挖掘、访问控制、业务风控、反欺诈、黑灰产识别、内容识别等安全能力。
- **云原生安全：**云基础设施及云平台的原生的安全能力，包括但不限于容器，无服务器 Serverless（FaaS 函数即服务），微服务，CI/CD，DevOps 等的安全性。
- **区块链原生安全：**包括数据层、网络层、共识层安全（即区块链可信基础设施），激励层、合约层、应用层安全，以及分布式数字身份等。
- **无线通信(5G/6G)原生安全：**通过身份认证安全、接入控制安全、通信安全、软件定义安全、数据加密等关键技术构建安全的 5G/6G 网络，实现“主动免疫，弹性自治，虚拟共生，泛在协同”的愿景。
- **物联网原生安全：**从云、管、端三个层面保障物联网平台/应用、网络和终端设备的安全性。
- **量子原生安全：**构建量子通信和量子计算的安全免疫系统，用量子安全应对未来的量子计算攻击，保障后量子世界的安全。

在数字经济高速发展过程中会不断的产生新兴技术，这些新兴技术在孕育新的业务形态的同时也会带来新的安全挑战和风险，进而导致新的法律和监管要求的诞生。这些变化最终必然会导致数字安全治理与合规的成本增加。

数字经济发展所需要的任何基础设施和基础技术（包括传统技术和新兴技术）都应具备原生安全能力，不过这对相关软硬件产业链和供应链的各环节都提出了更高的要求。

2.11.1 云安全

2.11.1.1 CS-CMMI 框架

CS-CMMI 全称是 Cloud Security Capability Maturity Model Integration，即云安全能力成熟度模型集成，由 CSA 大中华区牵头、亚太区与全球共同开发和研制的，把《CSA CSTR 云计算安全技术标准要求》和《CSA CCM 云控制矩阵》的技术能力成熟度模型，集成到一个治理框架中，根据 ISO/IEC 21827:2002 系统安全工程能力成熟度模型，以及 CSA《云计算安全技术要求》和 CSA《CCM 云安全控制矩阵》，形成云安全能力成熟度模型集成框架。该模型如图 2-5 所示。

图 2-5 云安全能力成熟度模型

2.11.1.2 CSA Cloud Controls Matrix(CCM) V4 框架

CSA Cloud Controls Matrix(CCM)云控制矩阵 V4 版包括 17 个控制域中的 197 个控制目标，全方位涵盖了云计算技术的安全领域。控制矩阵内构建了统一的控制框架，通过减少云中的安全威胁和弱点，加强了现有的信息安全控制环境，提供了标准化的安全和运营风险管理，并寻求将安全期望、云分类和术语体系，以及云中实施的安全措施等标准化。云控制矩阵可以用作对云计算实施的系统性评估工具，也可以作为云计算供应链中各角色与安全控制关系的指导。云控制矩阵的示例如图 2-6 所示。

图 2-6 云控制矩阵

2.11.2 NIST Big Data Architecture 框架

NIST 大数据参考架构是一种供应商中立的方法，可供任何旨在开发大数据架构的组织使用。NIST 大数据参考架构（Big Data Reference Architecture）如图 2-7 所示，代表一个大数据系统，由五个逻辑功能组件或通过互操作性接口（即服务）连接的角色组成，而管理、安全和隐私与所有五个组件交织。

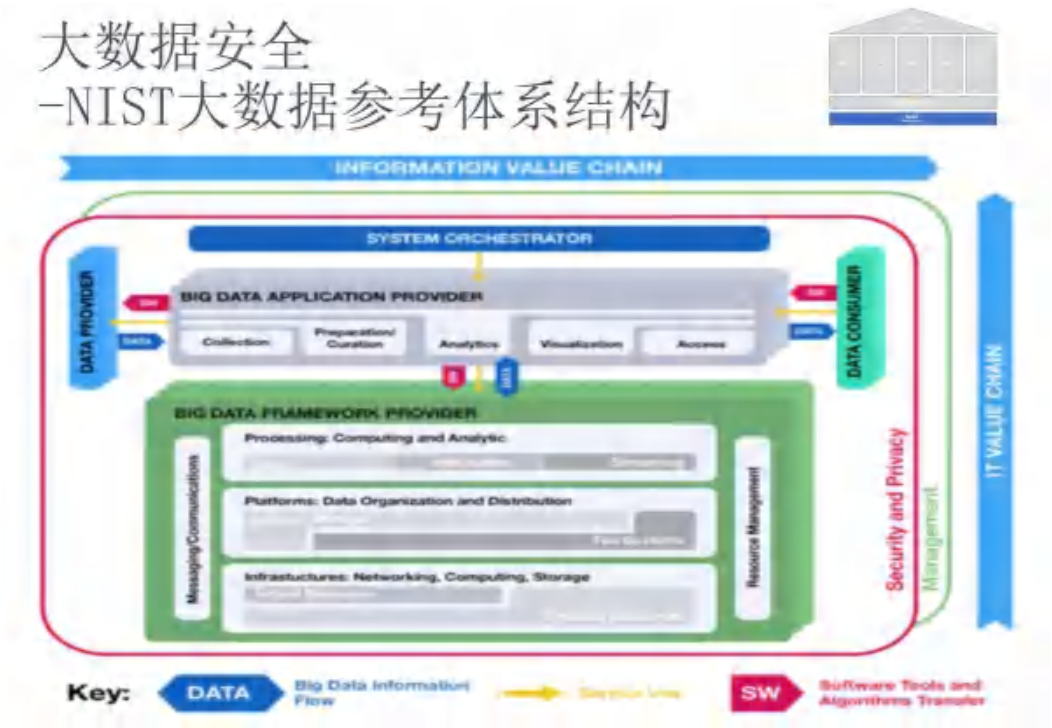


图 2-7 NIST 大数据参考架构

2.11.3 ICO AI 审计框架

人工智能应用程序可能会加剧现有的数据保护风险，引入新的风险，或者通常会使风险更难发现或管理。同时，由于人工智能应用的速度和规模，对数据主体的损害可能会增加。为了设计和实施有效的数据保护措施，组织需要能够理解和管理 AI 特有的关键风险领域。ICO 提出的 AI 审计框架草案（图 2-8），通过产生包括治理的技术（例如系统影响评估）和非技术（例如人类监督）组成部分的指导对话，并代表了标准化 AI 治理的重要里程碑。

图 2-8 ICO AI 审计框架草案

2.11.4 OT 框架

2.11.4.1. OT 框架

普渡模型，正式称为普渡企业参考体系结构（PERA），是工业控制系统（ICS）安

全的结构模型，涉及物理过程、传感器、监控、操作和物流，可见图 2-9。

图 2-9 普渡模型

普渡企业参考架构由西奥多·J·威廉姆斯（Theodore J.Williams）和普渡大学计算机集成制造联盟（Purdue University Consortium for computer integrated manufacturing）成员于 20 世纪 90 年代开发，定义了生产线中使用的不同级别的关键基础设施以及如何确保其安全。PERA 在引入时处于领先地位，如果正确实施，可以实现工业控制系统（ICS）或操作技术（OT）与 it 系统之间的气隙。以下是对不同级别的快速概述：

4/5 级-企业：这通常是我们今天所知道的 IT 网络，主要业务功能发生在这里。这是提供业务指导和协调制造操作的级别。企业资源规划（ERP）系统驱动工厂生产计划、材料使用、运输和库存水平。流行的 ERP 系统包括 Oracle、SAP、Microsoft 和 Epicor 提供的产品。这一级别的任何中断都可能导致数天甚至数周的停机，从而可能导致下游流程延迟或停止，从而造成重大收入损失。

3.5 级-非军事区（DMZ）：在过去十年中最近增加的一个级别，该级别包括安全系

统，如防火墙和代理，用于隔离或隔离 IT 和 OT 世界。这是 IT 和 OT 世界“融合”的地方，增加了 OT 系统的攻击面。许多工厂要么没有这一层，要么能力非常有限。自动化的兴起导致了更高的效率，这就增加了对 OT 和 IT 系统之间双向数据流的需求。这种 OT-IT 融合最终为正在加速数字化转型的公司创造了强大的竞争优势。

第 3 级-制造运营系统：这是在制造车间管理生产工作流的地方。基于操作系统（如 Windows）的定制系统用于执行批次管理、记录数据以及管理操作和工厂性能。该级别的系统称为制造执行系统（MES）或制造运营管理系统（MOMS）。MES/MOM 特定于正在加工/制造的产品。该层还由数据库或历史学家组成，用于记录操作数据。企业级和制造级之间的通信通常通过专用回程网络进行，连接到主数据中心或总部。与企业级一样，制造级的任何中断都可能导致数小时或数天的停机，这极有可能造成收入损失，因为它会影响整个制造厂。

2 级-控制系统：数据采集与监视控制系统（SCADA）软件用于监督、监测和控制物理过程。SCADA 可以从工厂的物理位置远程管理系统，而分布式控制系统（DCS）和可编程逻辑控制器（PLC）通常部署在工厂内。连接到 DCS 和 PLC 的人机界面（HMI）允许进行基本控制和监测，而 SCADA 系统聚合数据并发送到上游，以供第 3 级记录。PLC 通常没有键盘和监视器。远程终端装置（RTU）允许操作员登录 SCADA 系统。西门子、施耐德电气、ABB、GE Digital 和罗克韦尔自动化是 SCADA 系统的一些主要供应商。该层的设备和策略通常通过 modbus 和 dnp3 协议通信，数据二极管可以帮助增强安全性。

第 1 级-智能设备：通过过程传感器、分析仪、执行器和相关仪器，在此级别上进行物理过程的传感和操作。为了提高效率，传感器越来越多地通过蜂窝网络直接与云中的供应商监控软件通信。

0 级-物理过程：定义实际的物理过程。

2.11.4.2. ISA/IEC 62443 框架

该系列标准提供了一个灵活的框架，解决和减轻当前和未来的安全脆弱性在工业自动化和控制系统(IACSs)中导致的问题。ISA/IEC62443 标准适用于所有关键行业部门和关键基础设施，是美国网络安全框架不可或缺的组成部分。虽然 ISA/IEC62443 标准长达 1000 多页，但所述的核心网络安全原则却非常简单，并在 IT 和 OT 环境中得到了验证，能够有效应对网络安全风险。ISA/IEC62443 框架如下所示：

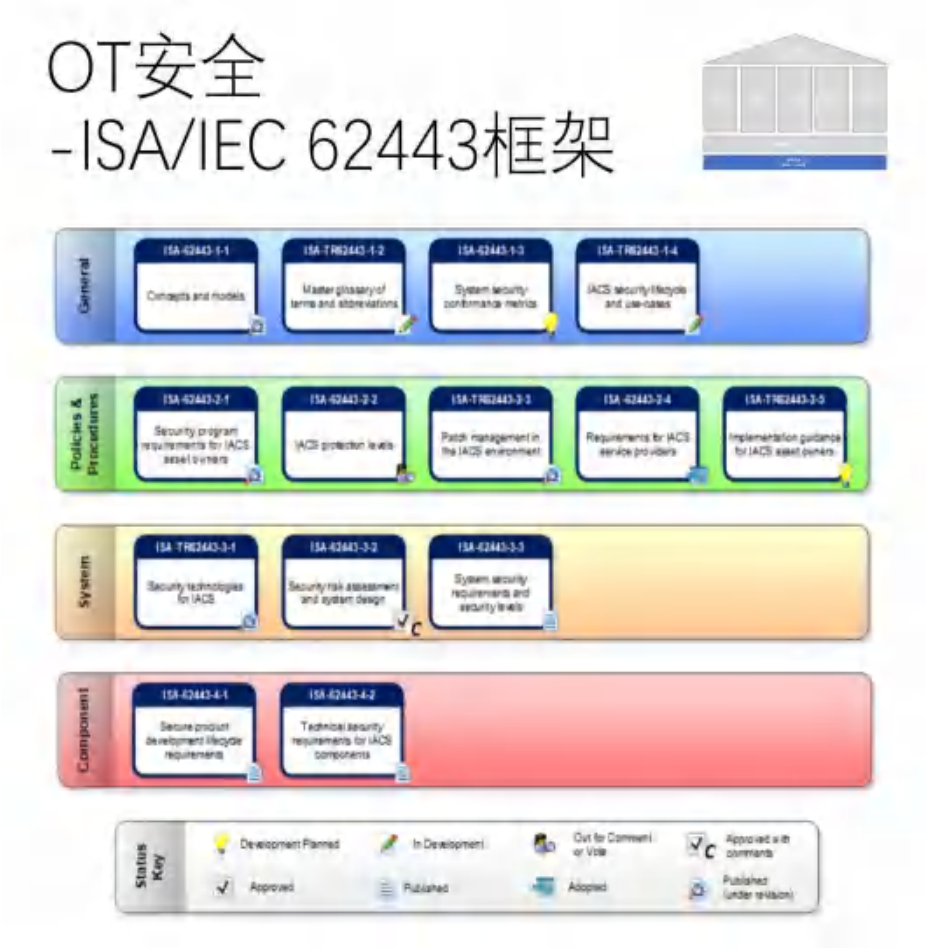
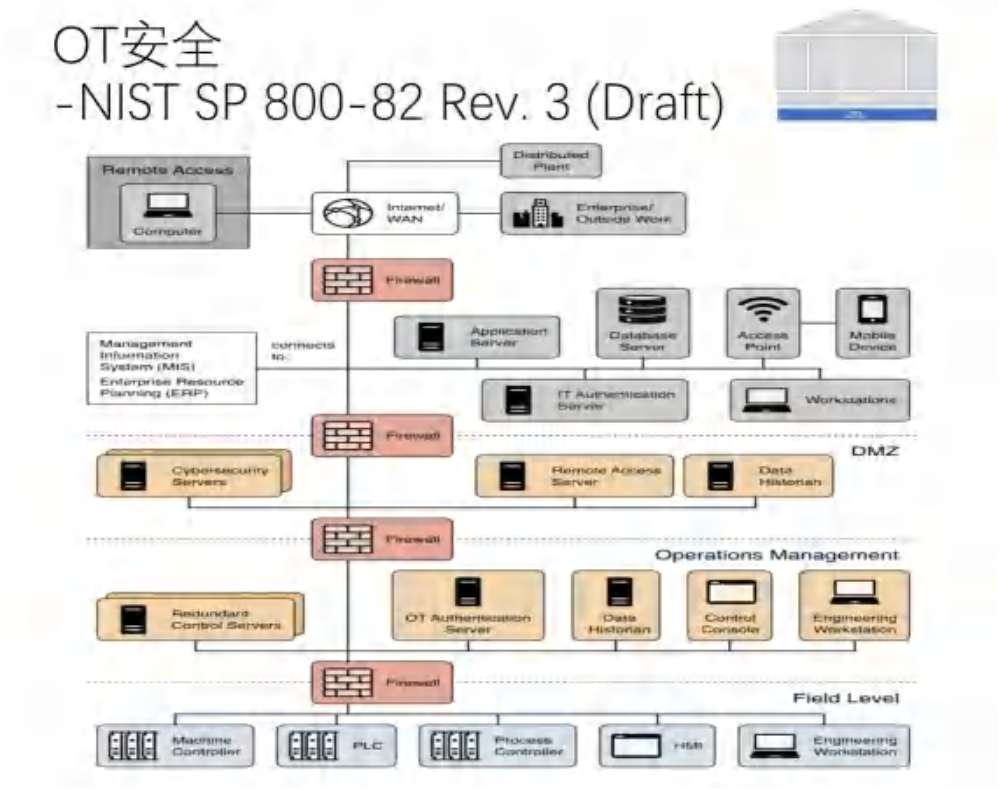


图 2-10 ISA/IEC62443 框架

2.11.4.3. NIST SP 800-82 Rev. 3 (Draft)

美国国家标准与技术研究院 (NIST)发布了 NIST SP 800-82 第 3 版的初步公开草案，如图 2-11 所示。该草案指导如何提高运营技术(OT) 系统的安全性，同时满足其性能、可靠性和安全要求。更新后的 NIST SP 800-82 文档提供了 OT 和典型系统拓扑的概述，识别了 OT 支持的组织使命和业务功能的典型威胁，描述了 OT 中的典型漏洞，并提供了推荐的安全保护措施和应对措施来管理相关风险。NIST SP 800-82 草案文件还概述了几种类型的标准 OT 系统，包括监控和数据采集 (SCADA)、分布式控制系统 (DCS)、可编程逻辑控制器 (PLC)、楼宇自动化系统 (BAS) 、物理访问控制系统 (PACS) 和工业物联网 (IIoT)。

图 2-11 NIST SP 800-82 Rev. 3 (Draft)



第三章 数字安全规则层

数字安全规则层是数字安全框架的战略指引，主要包含数字安全法律、数字安全治理、数字安全标准等内容。

3.1 数字安全法律

3.1.1 中国数字安全法律概览

一般认为，现行有效的中国数字安全主要法律和政策架构发轫于 2010 年前后[1]，以 2008 年工业和信息化部的重组和 2011 年国家互联网信息办公室的设立为标志。加之公安部门在此之前已经履行部分网络安全、信息安全监管职能。国家互联网信息办公室、工业

[1] 在此之前，中国数字安全领域的典型法律文件包括中国立法机关全国人大常委会制定的《关于加强网络信息保护的决定》，作为主要监管机构之一的公安部门制定的《计算机信息系统安全保护条例》等，一般认为以《网络安全法》为标志，中国的数字安全法律进入新阶段。但法治化始终是持续和渐进的，而非零散或突发的过程。

和信息化部和公安部初步统筹的互联网监管体制基本形成。自此数字产业与安全的法律政策进入快车道[2]，且这一法律化进程仍在持续。

图 3-1：中国数字安全法律体系[3]

3.1.1.1 《网络安全法》与《国家网络空间安全战略》

2017 年 6 月 1 日，《网络安全法》正式实施，确立了网信部门统筹，各部门在职责范围内各司其职的网络安全领域监管体制，通过设计一般网络与关键信息基础设施的运行安全，个人信息保护的信息安全的双重结构，奠定了当前和可预见未来一段时期中国数字安全立法政策的基本路径。

在《网络安全法》实施前后，2016 年 12 月，国家互联网信息办公室发布《国家网络空间安全战略》，不仅是中国在网络空间与数字安全领域的首份专门战略，同时构成了对《网络安全法》下促进网络安全产业和网络运行安全的直接回应和支撑。

与《网络安全法》的颁布同期，2015 年《中华人民共和国刑法修正案（九）》将网络犯罪立法作为其重要内容，对刑法中涉互联网安全的内容（特别是第 285 条至 287 条等

[2] 2009 年《中华人民共和国刑法修正案（七）》增设了非法获取计算机信息系统数据罪，非法控制计算机信息系统罪、出售、非法提供公民个人信息罪，并将提供侵入、非法控制计算机信息系统程序工具这类刑法理论上的帮助行为作为正犯行为入罪，增设提供侵入、非法控制计算机信息系统程序工具罪作为独立的罪名。从刑事法律角度实现了与国际上主要的打击和惩治计算机犯罪规定的对接。民事法律领域，2009 年《侵权责任法》也正式在立法层面确立了隐私权。

[3] 对于地方法规，中国在数字安全领域已有一些典型的地方性立法，例如 2021 年 11 月通过的《上海市数据条例》，在其行政区域内具有法律效力；对于强制性和推荐性标准，按照中国《标准化法》等规定，非强制性国家标准不具有法律上的直接强制力。为行文方便，除另有列明外所引述法律均为中华人民共和国法律。

关键条款）做了大量的补充和完善，增设了拒不履行信息网络安全管理义务罪、非法利用信息网络罪、帮助信息网络犯罪活动罪、编造、故意传播虚假信息罪，并对出售、非法提供公民个人信息罪进行整合，修改为侵犯公民个人信息罪。

3.1.1.2 《民法典》和《个人信息保护法》

2020 年 5 月，中国首部民事法律领域的基本法典《民法典》通过，并自 2021 年 1 月 1 日起施行。对网络空间与数字领域的最重要规制在于分别规定了隐私权的概念和个人信息的范畴，并适用了不同的权利义务和责任规范体系。

《民法典》与 2021 年 11 月 1 日起施行的《个人信息保护法》一并构成了当前中国个人信息保护的基础性法律，特别是后者全面建立了以知情同意为基本原则的个人信息处理规则（和除外）体系，进一步发展和细化了《网络安全法》和《民法典》的原则性规定，更具实际操作性，成为目前企业进行个人信息保护法律遵从与合规的起点[4]。此外，《电子商务法》等也对在线平台场景中的个人信息保护提出了专门规制，成为中国个人信息保护法律体系的重要组成。

3.1.1.3 《国家安全法》与《反恐怖主义法》

作为与《网络安全法》同时期的基本法律，《国家安全法》与《反恐怖主义法》在数据内容的规范性与合法性上也做出了规定，对危害国家安全的信息和恐怖主义、极端主义内容信息进行了合法性排除，可视为是对数字安全保障另一维度的观察与治理考量。

2020 年 6 月施行，并在 2022 年 2 月修订施行的《网络安全审查办法》（以下简称“《办法》”），即是同时体现《国家安全法》《网络安全法》，以及《数据安全法》等数字安全立法的产物。《办法》规定了两类触发网络安全审查的主要情形：（1）关键信息基础设施运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查（第 2 条）；（2）网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照办法的规定进行审查（第 16 条）。典型事件是网络安全审查办公室 2021 年 7 月对“滴滴出行”启动的网络安全审查[5]。

---

[4] 在《个人信息保护法》和《网络安全法》下，中国国家互联网信息办公室等监管机构制定了相当数量的个人信息保护的配套文件，如《APP 违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等等，限于篇幅本报告不再赘述。

[5] 2022 年 7 月，国家互联网信息办公室作出网络安全审查相关行政处罚的决定，对滴滴全球股份有限公司处人民币 80.26 亿元罚款，对滴滴全球股份有限公司董事长兼 CEO、总裁各处人民币 100 万元罚款。http://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm

3.1.1.4 《数据安全法》

2021 年 9 月 1 日起施行的《数据安全法》代表了中国数字安全领域法律政策的新努力，特别是数据分类分级保护制度、重要数据目录管理等都将成为监管和执法的新方向，也成为数字行业密切关注的新焦点。

围绕《数据安全法》，目前中国正在构造相应的配套制度体系，包括政务数据安全与开放、数据出境评估制度、数据安全审查、数字交易中介规则等等，以促进数字经济的安全、规范发展。目前部分配套制度已在征求意见或审议阶段，但具体落地内容和对数字经济和安全产业的影响尚有待观察[6]。

3.1.1.5 《密码法》和《关键信息基础设施安全保护条例》等

2021 年 9 月 1 日起施行的《关键信息基础设施安全保护条例》是《网络安全法》的重要配套制度，规定了识别和认定为“关键信息基础设施”的运营者的主要职责与义务。条例的主要特点是在规定国家网信部门统筹协调，公安部门主要负责，电信主管部门和其他有关部门在各自职责范围内分别负责的基本监管体系下，增加了行业、领域的保护工作部门的职责。

2020 年起施行的《密码法》在中国数字安全领域也极具鲜明特征，是中国继《电子签名法》后密码技术领域的又一基础性法律，特别是在《电子签名法》确立的电子签名和认证民事体系上，进一步将密码的认证功能延申到电子政务和关键信息基础设施等领域，也是国际上为数不多的专门针对密码进行全过程和综合规范的基础性法律。

2018 年 10 月通过《国际刑事司法协助法》，将我国涉外刑事司法协助上升至法律层面。针对执法跨境调取数据，该法第 4 条规定：“非经中华人民共和国主管机关同意，中华人民共和国境内的机构、组织和个人不得向外国提供证据材料和本法规定的协助。”该条的增加在于应对实践中有外国司法执法机关未经我国主管机关批准要求我国境内的机构、组织和个人提供相关协助的情况，其对于有效抵制外国的“长臂管辖”要求，维护数据主权的主张发挥了积极效用。同时，《数据安全法》《个人信息保护法》中均设置有对应该条规定的衔接性条款。

在数据相关投资、贸易歧视性措施的对等措施规制方面，还有《反外国制裁法》《出口管制法》，商务部《不可靠实体清单规定》以及《阻断外国法律与措施不当域外适用办法》等。

[6] 作为《网络安全法》到《数据安全法》的基础保障的网络安全等级保护制度，目前生效的主要文件是作为国家标准的《信息安全技术 网络安全等级保护基本要求》，有关数字安全相关标准的介绍，见本报告的数字安全标准章节部分。

3.1.1.6 数字安全的司法程序性和证据类法律规定

在数字安全的记录证据化领域，中国立法界和司法界主要通过修订相关司法程序规则的方式，努力跟上数字经济和产业发展的步伐。2019 年 12 月，最高人民法院发布了修正后的《最高人民法院关于民事诉讼证据的若干规定》，在民事诉讼领域对电子证据的范围进行了补充、完善，同时明确了电子数据的审查判断规则。在此之前的 2016 年 9 月，中国最高人民法院、最高人民检察院和公安部联合发布的《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》，以及公安部于 2019 年发布的《公安机关办理刑事案件电子数据取证规则》，均在刑事诉讼领域对电子数据证据从收集、提取、移送、展示、审查与判断等进行了全过程的规定。

这些对电子数据证据的程序性规定衔接了与《网络安全法》《个人信息保护法》《数据安全法》等规定的日志、记录的法律关系，增强了数字安全司法保障的力度和周延性。

3.1.1.7 其他典型法律文件

除此之外，中国数字安全领域的典型法律文件还包括《互联网信息服务算法推荐管理规定》和《汽车数据安全管理若干规定（试行）》等。这些法律文件虽然位阶在基本法律、行政法规之下，但在一些特定领域进行了更具颗粒度的制度规范，体现了数字产业发展与安全关注的阶段性方向。

《互联网信息服务算法推荐管理规定》对“推荐类算法”进行了法律分类，特别规定了对具有舆论属性或者社会动员能力的算法推荐服务提供者，应当通过互联网信息服务算法备案的备案制度[7]。后者则首次从规范性法律文件层面，对《数据安全法》规定的何为重要数据做出了汽车领域的明确：（1）军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；（2）车辆流量、物流等反映经济运行情况的数据；（3）汽车充电网的运行数据；（4）包含人脸信息、车牌信息等的车外视频、图像数据；（5）涉及个人信息主体超过 10 万人的个人信息；（6）监管机构确定的其他数据。

2022 年 5 月《数据出境安全评估办法》通过，自 2022 年 9 月 1 日起施行。该办法规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动。数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息，在触发相应条件时需要进行法定安全评估。数据出境安全评估坚持事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，保障数

[7] 互联网信息服务算法备案系统：https://beian.cac.gov.cn/#/index，2022 年 3 月上线。2022 年 4 月，中国网信部门等开展算法综合治理监管活动。

据依法有序自由流动，与《个人信息跨境处理活动安全认证规范》《个人信息出境标准合同》等一并构筑了中国数据出境监管规则体系。

3.1.2 主要国家和地区的数字安全法律概览

在讨论中国数字安全法律时，不应孤立地看待和评价其法律政策的本土化特征，而应将中国围绕数字安全的法律置于全球背景下进行比较参照，并观察同一时期主要国家、地区法律政策的动向，才能从整体性和全球化的高度得出数字经济发展与安全的总体、局部水平和进展情况。

3.1.2.1 欧盟个人数据与非个人数据保护的概括与进展[8]

欧盟 2018 年生效的《通用数据保护条例（GDPR）》是目前各国都最为关注的个人信息保护领域的法律，GDPR 详细的个人数据（信息）主体权利（特别是其创设的可携带权、被遗忘权等等）和个人数据控制者义务规定均为各国在个人信息保护领域立法所参考和讨论，并对很多国家和地区的法律进程产生了深远影响。GDPR 与 2018 年 11 月颁布的《非个人数据自由流动条例》共同形成了欧盟单一数字市场和协调数据治理的统一框架基础。

但这并不意味着欧盟在数字领域立法的终点，欧盟在 2020 年 12 月再次推出《数字服务法》与《数字市场法》，2022 年 1 月欧洲议会率先通过《数字服务法》，为对数字平台的经营活动监管提供法律工具。《数字市场法》则面向定义为“守门人”的互联网平台企业，旨在进一步推动数字市场的开放与公平。这与中国国务院反垄断委员会 2021 年发布的《关于平台经济领域的反垄断指南》，以及《个人信息保护法》中的“提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者”有类似之处。普遍的观察认为，这些规定将在新成立的欧洲数字服务委员会（European Board for Digital Services）支持下，制定更为完整和充分的数字平台行为准则和技术标准。整体上，欧盟法律中突出了对个人数据主体和市场公平竞争秩序的保护，对违法主体可能处以高额的处罚尤为引人关注。

在欧盟 GDPR 监管实践中，欧盟数据保护委员会（EDPB）等监管主体对内发布了大量的指导文件，持续细化和澄清个人数据主体相关权利的内容，对外则通过“充分性认定”等方式，实现个人数据在欧盟和经充分性认定的国家（例如已与日本、韩国等达成协定）之间自由流动。

[8] 值得注意的是，欧盟层面的法律文件应通过国内法转化后对其成员国具有约束力。为简明起见，此部分不再罗列欧盟各成员国的相应文件。

英国在 2020 年 12 月宣布完成“脱欧”后，在数字经济领域进行了法律重塑的部分工作。2022 年 5 月公布的《数据改革法案》宣称，对英国现有的《通用数据保护条例（GDPR）》和《数据保护法案（Data Protection Act）》进行必要改革，形成英国版的数据保护框架。这些举措都将使未来英国的数字安全法律、政策具有不同于欧盟的鲜明特点。

3.1.2.2 美国的州立法进展、典型案例，以及美欧相关协定

美国在联邦和州层面的数字安全法律具有相当长的延续历程。2010 年之后相关领域的主要进展包括：（1）为落地 2014 年《网络安全促进法》和行政令，美国国家标准与技术研究所（NIST）发布了《提升关键基础设施网络安全框架》，成为目前各国在进行关键（信息）基础设施保障中的重要参考；（2）2015 年以年度《综合财政拨款法》的形式通过《网络安全信息共享法（CISA）》等一系列法案，推动联邦层面的网络和数字安全，延续了《国土安全法》《爱国者法案》《联邦信息安全管理法》《外国情报监控法案》等确定的立法思维；（3）2018 年 3 月《澄清合法使用境外数据法案》（又称《云法案 CLOUD Act）》）通过，法案突破了基于传统多边或双边司法互助协定的执法数据跨境访问模式，部分重塑了数据跨境提供和披露的内外规则，对各国的跨境数据调取法律政策的调整都产生了重大影响。

在个人信息保护领域，2018 年 6 月加利福尼亚州通过的《消费者隐私法案（CCPA）》成为美国隐私与个人信息保护领域的州立法典范，也是与 GDPR 相当的一部重要法律。这一领域的其他州立法还包括弗吉尼亚州、科罗拉多州等相关立法。与前述趋势不同，2021 年 7 月，美国统一法律委员会投票通过了《统一个人数据保护法（UPDPA）》，这是一项旨在统一州隐私立法的示范（不具有强制性，需要由州立法机构引入和转化为州法）法案，法案为隐私与个人信息监管提供了一个替代方案。这也体现出个人信息与隐私法律保护问题的复杂性与持续性。

此外，欧洲法院在先后裁决 2016 年签署的《隐私盾协议》、2000 年签署的《安全港协议》无效后，美国与欧盟之间围绕数据安全流动如何更新“数据隐私框架”，不仅是美国数据跨境法律需要解决的头等问题，也为包括中国在内的各国数字安全领域政策法律所关注。

3.1.2.3 俄罗斯

从《国家信息安全学说》（1994 年筹划，2000 年制定，2016 年更新）开始，俄罗斯开始逐步构建起网络安全防护法律体系，《俄罗斯联邦通讯法》《〈俄罗斯联邦关于信息、信息技术和信息保护法〉修正案》（两者合称《主权互联网法》）等被公认为是俄罗斯在网络安全法体系方面的基本框架。

2018 年 1 月开始施行的《俄罗斯联邦关键信息基础设施安全法》是近年来俄罗斯在网络与数字领域最为重要的关键性法律，其旨在建立并调整俄罗斯联邦关键信息基础设施安全保障领域的法律关系。2019 年 11 月，《主权互联网法》颁布生效，两者共同支持了包括与国际互联网络“断网”测试演习、禁止关键信息基础设施（CII）设施使用外国软件（以总统令形式确立）等在内的一系列重大网络活动。整体上，俄罗斯的网络与数字安全法律政策具有独立性特点，这可能与其地缘政治等因素有关。

3.1.2.4 日本与韩国

2014 年 11 月，日本国会批准了《网络安全基本法》，首次从法律上定义了网络安全，设立网络安全战略总部负责制定网络安全战略并保障其实施。在个人信息保护领域，《个人信息保护法》于 2003 年 7 月制定，2005 年 4 月 1 日正式实施。2020 年多次修改后的修正案于 2022 年 4 月 1 日起正式实施。修正案回应了近年来全球范围内个人信息保护与冲突的个案和争议，在适用范围、作为独立监管机构的个人信息保护委员会（PPC）的职责和数据跨境规则等方面都进行了扩展。总的观察认为，日本对个人信息的法律保护极为重视，在个人信息跨境流动方面与欧盟立场相近。

其他方面，日本还通过出台和修订诸如《电信事业法》《防止不正当竞争法》《禁止未经授权的计算机访问法》等法律对电信运营商义务、数据交易、打击网络犯罪进行明确，也可视为在网络安全基本法框架下的典型细分做法。

从 2007 年《促进使用信息通信网络及信息保护相关法》和 2011 年《个人信息保护法》算起，韩国持续推动个人信息保护法律化，截至 2020 年，韩国国会已经通过（和修订）了旨在明确收集、利用的个人信息范围和保障数据产业发展的《公共信息和公共数据门户服务指南》《公共数据公开与利用法案》《个人信息保护法（PIPA）》、《信用信息保护法》《位置信息的保护与利用相关法》等相对完整的监管体系。

在信息技术和信息（数字）基础设施安全保障领域，韩国早在 2001 年通过《信息通信基础设施保护法》（2007 年开始持续修订），2015 年 3 月制定《云计算发展与用户保护法》，2021 年 8 月修正《电信业务法》，为推动数字经济的公平和安全发展提供法律依据。

3.1.2.5 新加坡

新加坡个人信息保护领域的基础性法律是 2012 年通过的《个人数据保护法》，在该法下构建了包括保护、通知、执法等一系列配套规则，并于 2020 年 11 月 2 日通过了《个人数据保护法》的修正法案。

2013 年《反计算机滥用和网络安全法》《电子交易法》修订后，新加坡近年来在网络与数字安全领域的主要法律成果是《网络安全法》，该法于 2018 年 2 月议会通过，是落实新加坡网络安全战略的重要举措，旨在建立关键信息基础设施所有者的监管框架、网络安全信共享机制、网络安全事件的响应和预防机制、网络安全服务许可机制，为新加坡提供综合、统一的网络安全法律基础框架。

此外，新加坡对《统计法》等细分领域的法律进行调整，为保障和推动数字经济和人工智能技术发展、智慧城市建设提供了依据，具有鲜明的地域特征。

3.1.2.6 其他

在 2010 年至 2020 年之间，国际上主要的国家和地区都在网络安全、数字治理等领域进行了法律布局，并先后颁布了“网络安全”“个人信息保护”等主题或类似法律。除前述法律外，还包括印度《信息技术法》（2000）和《个人数据保护法》（2019）、巴西《个人数据保护法（LGPD）》（2020）、肯尼亚《个人数据保护法》（2019）等等。另外一些英美法系国家，如加拿大则与美国相似，在个人信息保护、新技术规范等领域的法律呈现碎片化和案例法的特点。

从法律调整范围上看，目前各国在网络与数字安全领域的法律基本都涵盖了个人信息保护、关键（信息）基础设施保护、网络内容监管（侧重各有不同）、反不正当竞争和反垄断、（虚拟货币、密码、云计算、人工智能、推荐算法、量子计算等）新技术新业态促进与规制等等。

3.1.3 国际公约、多边与双边协定

全球范围内看，在数字安全领域的法律与政策推动，也与国际组织、多边和双边协定等方式密切相关。特别是在联合国框架内，各国围绕数字经济与转型的诸多问题，形成了相当丰富的公约、协定、协议等法律文件，中国在其中亦发挥有重要作用。

3.1.3.1 联合国

联合国及联合国下设机构在网络与数字安全领域形成了诸多法律类文件和成果，涵盖了从个人信息到行业数据，从数字经济安全到打击网络犯罪的各个方面。简要列举如下：

个人信息领域，联合国对个人信息保护的关注可以追溯到 1948 年的《世界人权宣言》《宣言》成为全球和区域层面人权法的恒久基础。其他典型文件包括 1990 年《个人资料保护指南》所确立的十项原则和相关文件；数字经济和行业数据领域，联合国大会 1996 年 12 月通过的《电子商业示范法》是及其重要的服务贸易法律文件，其所定义的“数据电文”等基础概念为各国所援引，推动了新千年以来各国电子商务和数字经济的立

法化活动，下设机构自动驾驶车辆工作组（GRVA）在 2019 年通过《自动驾驶汽车框架文件》等智能网联汽车领域强制性法规，体现了在细分行业领域联合国关注事项的进展；联合国大会 2002 年 12 月通过《创造全球网络安全文化的要点》，2015 年提出《2030 年可持续发展议程》，2021 年联合国贸易和发展会议发布年度《数字经济报告》，这些文件呼吁创造全球网络安全文化，通过全球数据治理框架解决数据跨境流动监管法律冲突问题，拥抱数字经济的变革与调整；而在网络犯罪领域，2021 年 5 月，第 75 届联合国大会通过关于打击网络犯罪公约谈判安排的决议，并于 2022 年 1 月正式启动，这是自 2001 年布达佩斯《网络犯罪公约》（Cyber-crime Convention，又译《打击网络犯罪公约》）之后，国际上针对网络安全犯罪的打击、惩治的最为重要的法律活动。

为应对日益复杂的数字安全问题，联合国通过信息安全开放式工作组（UN OEWG）和政府专家组（UN GGE）的安排，进行联合国框架下的网络空间国际规则制定，至 2021 年已经取得阶段性重要进展，这些努力也将继续贡献联合国体系下的数字安全治理法律和可持续发展理念。

3.1.3.2 OECD 与 APEC 在数字安全领域的典型文件

1980 年的经济合作与发展组织（OECD）《关于隐私保护和个人数据跨境流动的指导原则》列举的八项原则（2013 年更新），成为包括欧盟 GDPR、亚太经济合作组织 APEC 等个人信息保护法律活动的早期渊源。除该原则外，OECD 还针对密码技术提出了《密码政策指南》八项原则（1997）、就各国网络政策建议的《网络政策制定原则的指南》（2011）、在人工智能领域于 2019 年 5 月发布了《人工智能原则》等，对其成员国内部的法律协调起到了极其重要的作用。

亚太经济合作组织（APEC）最为重要的网络与数字安全法律文件是构建了一整套跨境隐私规则体系（CBPR）。2005 年 APEC 制定了包括隐私原则和实施指南在内的隐私框架，提出九项个人信息保护原则，2011 年 CBPR 经表决通过（2016 年修订）。CBPR 体系建立了一套由政府支持的基于自愿和可执行的隐私保护认证机制。

3.1.3.3 WTO

WTO 构筑的国际贸易协定体系文件主要包括关税及贸易总协定（GATT）、服务贸易总协定（GATS）、技术性贸易壁垒协定（TBT）和与贸易有关的知识产权协定（TRIPS）等。作为国际货物、服务贸易领域最重要的组织和体系设计者，尽管对数字数据跨境的产品贸易是属于货物贸易还是服务贸易存在一定的争议，但 WTO 仍在努力实现向贸易数字化转型，与数字安全相关的议题主要集中于数字跨境规则（一般原则和为国家安全的除外情形）的设定，近年来这一领域的讨论始于 2019 年通过的《关于电子商务的联合声

明》，相关工作仍在继续。

3.1.3.4 《区域全面经济伙伴关系协定（RCEP）》

2020 年 11 月 15 日，中国与东盟十国及日本、韩国、澳大利亚及新西兰共同签署《区域全面经济伙伴关系协定（RCEP）》，其中包括了对区域内国家的贸易、经济及社会的数字化发展如何建立数据治理框架和强化打击网络犯罪的合作等内容的考量，并特别的将电子商务作为专章进行规定，设定了消费者和个人信息保护、垃圾信息治理、网络安全保护、电子签名、跨境电商与传统制造业融合等内容。

对于 RCEP 面临的区域内各国的经济发展水平、信息化水平和网络安全能力的差异问题，观察认为，一方面差异的存在为保障数字安全的基线保障提出挑战，另一方面也为各国促进数字经济发展提供了数字技术的各种可能。

3.1.3.5 《全面与进步跨太平洋伙伴关系协定（CPTPP）》

2018 年底正式生效的《全面与进步跨太平洋伙伴关系协定（CPTPP）》是数字经济领域及其重要的多边协定，与 RCEP 类似，CPTPP 也专章规定了电子商务等内容，对网络安全、数据跨境等都设定了相应的规则要求。2021 年 9 月 16 日，中国正式提出申请加入。

3.1.3.6 其他区域组织和法律文件

2016 年 G20 杭州峰会通过了《二十国集团数字经济发展与合作倡议》。这是“数字经济”重要文件首次亮相国际治理舞台，明确提出应“提高基于信息通信技术的关键基础设施的安全性，以使信息通信技术继续成为加快经济发展的可靠动力”，“通过确保尊重隐私和个人数据保护，树立用户信心，这是影响数字经济发展的关键因素”。2017 年，G20 为数字经济的安全与发展首次专门设定了数字经济部长会议，2021 年成立专门的数字经济工作组，其短期目标包括在网络安全上达成共识，以实现包容性数字转型。

上海合作组织于 2007 年批准《上海合作组织成员国保障国际信息安全行动计划》，随后推出了多部法律文件，特别是 2019 年通过《上合组织成员国关于数字化和信息通信技术领域合作的构想》，并于 2020 年签署《上海合作组织成员国元首理事会关于数字经济领域合作的声明》，体现了对数字经济领域的高度关注。

2020 年 6 月新加坡、智利和新西兰初始完成《数字经济伙伴关系协定（DEPA）》的在线签订。DEPA 是数字贸易领域最早的单独协定，针对性的协调数字贸易合作，制定数字贸易规范，以为全球数字经济制度安排提供模板。中国于 2021 年 11 月 1 日正式提出申请加入。

3.1.3.7 中国《网络空间国际合作战略》与《全球数据安全倡议》

中国在上述涉及数字安全的多边和双边体系下，正通过参与主办、提出方案、协商斡旋等方式贡献中国这一最大发展中国家的独特价值。近年来特别是通过《网络空间国际合作战略》与《全球数据安全倡议》[9]等文件，提议和推动网络空间命运共同体这一命题的建设。在 2017 年《网络安全法》颁布前后，《网络空间国际合作战略》同期发布，2020 年 9 月《全球数据安全倡议》提出，为全球数字治理不断提供中国方案。

数字安全领域的主要法律一览表如下[10]：

	个人信息/隐私保护	关键（信息）基础设施与政府信息	数据与数字经济；信息与网络安全技术	网络内容与执法协助
中国	《个人信息保护法》《民法典》	《关键信息基础设施保护条例》	《网络安全法》《数据安全法》《密码法》《数据出境安全评估办法》	《国家安全法》《反恐怖主义法》
美国	《消费者隐私法案》（CCPA）《统一个人数据保护（示范）法》（UPDPA）	《国土安全法》《爱国者法》《外国情报监控法》《联邦信息安全管理法》	《网络安全促进法》《网络安全信息共享法》《国家量子倡议法》《综合财政拨款法》《数字千年版权法》	《通信协助执法法案》《澄清合法使用境外数据法案》（《云法案》）、《外国投资风险审查现代化法》
欧盟	《通用数据保护条例》《非个人数据自由流动条例》	《网络安全法》《网络与信息安全指令》（NIS/NIS2）	《数字服务法》《数字市场法》	《数字内容合同指令》
俄罗斯		《俄罗斯联邦关键信息基础设施安全法》	《国家信息安全学说》	《主权互联网法》
日本	《个人信息保护法》		《网络安全基本法》《防止不正当竞争法》	《电信事业法》《禁止未经授权的计算机访问法》
韩国	《个人信息保护法》	《促进使用信息通信网络及信息保护相关法》《信息通信基础设施保护法》《公共信息和公共数据门户 服务指南》《公共数据公开与利用法案》	《云计算发展与用户保护法》《电信业务法》	《信用信息利用与保护法》《位置信息的保护与利用相关法》
新加坡	《个人数据保护法》		《电子交易法》《统计法》	《反计算机滥用和网络安全法》

表 3-1 数字安全领域的主要法律

[9] 一般认为，多边和双边协定、协议属于对签署国有约束力的法律文件，倡议和战略不具有强制约束力。尽管倡议类文件可以作为自我要求和承诺，但不应视为具有法律意义上的约束力。

[10] 按照重要性原则，列出各国主要的法律文件，但非全部法律。

3.2 数字安全治理

数字安全治理核心是为数字经济服务与赋能，保证数字经济的安全、合规、公平、效率，让所有数字经济参与者都能够更加积极主动的去拥抱数字经济，充分利用各种数字化手段创造价值并享受价值。可以说，数字安全治理是数字化的支柱与基石。数字安全治理的效果，将使得无论是关键基础设施行业，还是个体公民，都能够安全放心的使用数字化产品与服务，共创数字时代安全、繁荣、美好的未来。

数字安全治理属于组织治理的一部分，帮助组织在实现数字化转型过程中有效对抗各类数字安全风险，实现平滑过渡；保障组织在数字化转型后充分享受数字化带来的效率与收益，并以合理的成本控制数字安全风险。其驱动力主要来自于两个方面：

- 合规、安全、隐私要求。满足组织所在地区与国家有关数字安全法律法规的要求，例如欧盟的《通用数据保护条例（GDPR）》《数字服务法案》《数字市场法案》；以及中国的《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《中华人民共和国电子商务法》《中华人民共和国电子签名法》等；
- 组织自身运营要求。数字经济时代，数字资产与设施已经成为组织基本生产要素与核心竞争力，因此保护好所拥有的数字资产是组织经营的基础，良好的安全治理可以协助组织增加利润，控制成本。同时，组织的最终客户也会对组织的数字安全建设提出要求，一个自身存在严重数字安全风险的组织无法为其最终客户提供安全的业务，易导致客户满意度下降及客户流失。

数字安全治理确保整个组织对数字安全建设和运营达成共识，确保组织数字资产能够得到有效的保护，节约资源，创造价值。数字安全治理涵盖了战略层与执行层：

- 在数字安全战略层面，数字安全治理主要关注于董事会和高层管理者如何对待数字安全，并形成数字安全治理战略，数字安全治理战略必须与组织数字化目标与愿景一致，协调多方利益，强调多方共同参与，从而获得关键决策人支持，获取预算与人力支持，并形成清晰、明确、可执行、系统化、基于风险评估的数据安全治理长期规划。
- 在数字安全执行层面，数字安全治理主要关注于如何建立、实施、运行、改进数字安全管理体系，结合组织数字化现状与远景，制定行之有效的治

理规则与过程行动计划，包括网络安全计划、信息安全计划、数据安全计划、身份安全与隐私保护计划、元宇宙安全计划等等，用以缓解/遏制当前及未来所面临的各种数字化安全威胁与风险。

数字安全治理无论是对于中心化的信息互联网安全、网络空间安全(Cybersecurity)，还是对去中心化的价值互联网安全、元宇宙安全，都应该形成自上至下的框架，包括概念、逻辑、物理、组件、运营，并在执行层面形成包括战略&规划，设计，执行，管理&度量的完整流程。

数字安全治理主要工作包括：

- 制定组织数字安全战略与目标，包含预算与人力资源投入计划，由组织最高管理层批准执行。
- 制定治理、风险管理和合规性（GRC）框架，框架首先要满足数字安全相关法律、法规、条例监管要求（见 3.1 节）。法律法规通常以提出监管要求为主，在具体执行层面，可以参考组织所在区域、国家、行业相关数字安全标准与最佳实践制定安全框架，例如 GB/T 22239-2019 信息安全技术、网络安全等级保护基本要求、ISO/IEC 27002:2022 信息安全、网络安全和隐私保护-信息安全控制等标准；以及 TOGAF、COBIT、SABSA、NIST CSF 网络安全框架等。
- 风险与业务影响评估：所有数字资产（网络、计算、存储、数据、应用、服务）都需要通过业务影响评估（BIA）明确其安全风险与安全需求，可以参考 ISO 31000：2009 风险管理–原则和指南进行评估。
- 数字安全体系建设：基于风险评估结果进行安全体系规划、设计、实施，可参考 ISO/IEC 27002:2022 标准，选择并部署适合自身需求的控制措施。
- 数字安全体系运营与持续改进：可参考 ISO/IEC 27002:2022 标准内容，按照 Plan（计划）-Do（执行）-Check（检查）-Act（行动）循环对组织的数字安全系统进行持续评估与优化。

数字安全治理框架按适用性范围可以划分为通用领域框架，以及特定领域框架。通用领域常见数字安全框架有：

- GB/T 22239-2019 信息安全技术：网络安全等级保护基本要求。
  - 技术要求：涵盖安全物理环境 、安全通信网络 、安全区域边界 、安全计算环境 、安全管理中心等方面的要求。

- 管理要求：涵盖安全管理制度 、安全管理机构 、安全管理人员 、安全建设管理 、安全运维管理等方面的要求。

- ISO/IEC 27002:2022 信息安全、网络安全和隐私保护-信息安全控制：信息安全管理体系 (ISMS)标准，旨在通过明确的管理控制满足信息安全需求，包含如下四个方面的控制措施：
  - 组织安全控制
  - 人员安全控制
  - 技术安全控制
  - 物理安全控制
- TOGAF（企业架构标准）：从安全、隐私和运营风险角度开发和整合企业安全架构，以有效和高效的方式实现业务目标。TOGAF 核心部分的架构开发方法（ADM）为开发企业架构提供了一个经过测试且可重复的过程，包括建立架构框架、开发架构内容、过渡和治理架构实现相关的活动，以有效和高效的方式实现业务目标。

图 3-2 ADM 架构开发生命周期（图中内容摘自 TOGAF Version 9 官方介绍文档）

[11]

TOGAT ADM 强调企业安全架构并不是孤立存在的，它是企业的一部分，应该与企业整体架构集成。虽然 IT 架构师往往主要关注系统如何工作，而安全架构师主要关注系统可能如何失败，但安全架构设计应该被尽可能早的引入整体架构设计之中。

安全架构主要关注领域包括：认证、授权、审计、保障、可用性、资产保护、安全策略管理、风险管理等方面内容。

典型的安全架构组件包括：关于数据/信息资产处理的业务规则、书面和发布的安全策略、编码数据/信息资产所有权和保管、风险分析文档、数据分类政策文件等等。

- COBIT（信息及相关技术控制目标）：提供了一个全面的框架，可帮助组织实现 IT 治理和管理目标。
- Sherwood Applied Business Security Architecture (SABSA)：介绍如何开发以风险驱动的企业信息安全和信息保障体系结构以支持关键业务计划的层次化方法；SABSA 认为许多组织存在的问题在于信息安全解决方案通常是在战术层面而非战略层面上设计、获取和实施的，并且每个解决方案都是独立设计,不能保证它们之间的兼容性和互操作性。避免这些问题的一种方法是开发企业安全架构，该架构由业务驱动，描述了技术和程序解决方案之间通过结构化相互关系支持业务的长期需求。如果架构要成功，那么就必须提供一个合理的框架，在这个框架内可以根据安全解决方案的选择做出决策。决策标准应来源于对业务需求的透彻理解，包括：降低成本需求、模块化、可扩展性、易使用性、内部和外部互操作性、与企业 IT 架构及其遗留系统的集成，等等。SABSA 模型基于著名的 Zachman 框架，用于开发企业架构模型，以建筑物设计为参考设计了六层架构层次化模型，每一层都代表了建筑设计、建造和使用过程中不同参与者的观点，用于辅助组织开发安全架构。一个组织的安全架构设计可以以建筑师视角为参考， 分别从业务视角、架构视角、设计视角、建设者视角、实施者视角、服务和管理视角出发进行业务、概念、逻辑、物理、组件、安全服务管理架构设计；SABSA 生命周期包括战略与规划、设计（包括逻辑、物理、组件和服务管理

[11] TOGAF9: www.opengroup.org/togaf

架构设计）、实施、管理和衡量四个阶段。

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Service Manager's View	Security Service Management Architecture

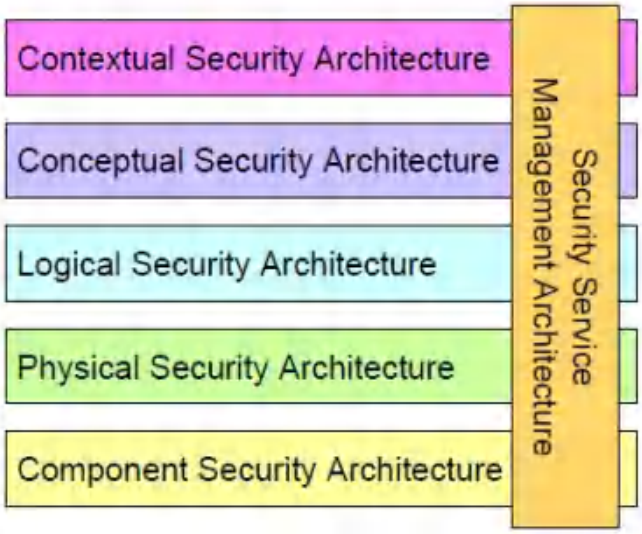


图 3-3 安全架构的 SABSA 模型[12]

- NIST 网络安全框架（CSF）:包含用于管理网络安全相关风险的标准、指南和最佳实践，该框架是一种基于风险的网络安全风险管理方法，由三部分组成：框架核心、框架实现层和框架概要。每个框架组件都加强了业务/任务驱动因素与网络安全活动之间的联系。框架核心部分定义了包括识别、保护、检测、响应、恢复在内的核心功能。

数据治理领域相关的数字安全框架有：

- ISO/IEC 38505 系列标准：该系列标准提出了数据治理框架（包括目标、原则和模型），以及数据治理的“E（评估）-D（指导）-M（监督）”方法论。
- DGI（国际数据治理研究所）数据治理框架：采用 5W1H 设计原则，分为人员与组织架构、规则、治理流程三个层面，关注如何管理数据，

[12] SABSA:https://sabsa.org/sabsa-white-paper-download-request/

实现数据价值，最小化成本和复杂性，管理风险以及确保遵守不断增长的法律、法规和其他要求。

- DAMA（国际数据管理协会）数据管理模型：数据治理是对数据管理的高层计划与控制，在数据安全管理方面，强调确保隐私、保密性和适当的访问权限等。
- Gartner DSG 数据安全治理框架：Gartner 认为数据安全治理是信息治理的一个子集，通过明确的数据策略和流程来保护公司数据，Gartner 将数据治理分为四个部分：规范、计划、建设和运营，定义了企业数据治理四个阶段重点应关注的内容。
- 第三方支付行业 (支付卡行业 PCI DSS)数据安全标准：适用于任何接受、传输或存储持卡人数据的公司，从信息安全管理体系、网络安全、物理安全、数据加密等方面提出了安全基线要求。
- IBM 数据治理统一流程：IBM 提出数据治理统一流程（The IBM Data Governance Unified Process），描述了面向数据治理从业者的统一流程，对基于 IBM 产品、服务的最佳实践实施数据治理的 14 个步骤进行了解释说明。

隐私保护领域相关的数字安全框架有：

- 微软隐私、保密和合规性框架（Data Governance for Privacy, Confidentiality and Compliance，DGPC）：围绕人员、流程和技术等能力领域，帮助组织更好的进行数据安全风险控制；DGPC 框架创建了一个环境，可以识别对隐私的威胁，包括不与网络安全威胁重合的隐私威胁，例如在收集何种类型的个人信息以及如何使用、处理和共享这些信息方面侵犯客户的选择和同意权；DGPC 框架可以与组织现有的 IT 管理和控制框架（如 COBIT）以及安全标准（如 ISO/IEC 27001/27002 和支付卡行业数据安全标准（PCI DSS））协同工作。DGPC 框架围绕三个核心能力领域组织：人员、流程和技术。
  - 人员：数据治理流程和工具的有效性取决于使用和管理它们的人。
  - 流程：首先各种数据安全相关规定必须满足权威文件要求（法规、条例、标准、公司政策和战略文件）；下一步是定义指导原则和政策以满足这些要求；最后组织应识别特定数据流中对数据安全、

隐私和合规性的威胁，分析相关风险，并确定适当的控制目标和控制活动。

- 技术：Microsoft 开发了一种方法分析特定的数据流，并识别信息安全管理系统和/或控制框架更广泛的保护措施可能无法解决的剩余风险。这种方法涉及填写一份称为风险/差距分析矩阵的表格，该表格围绕三个要素构建：信息生命周期、四个技术领域（基础设施安全、身份及访问控制、信息保护、审计和报告）以及组织的数据隐私和保密原则。

随着组织管理越来越多的机密数据，他们在保护数据免受盗窃、滥用或未经授权的披露方面面临着越来越复杂的挑战。DGPC 通过提供一种整体方法识别针对数据隐私、安全和合规的数据流特定威胁，并通过有效和高效的方式解决剩余风险，补充了现有的安全标准和控制框架。

- NIST 隐私框架：通过企业风险管理提高隐私保护能力，帮助企业或组织保护个人隐私，以便其更好遵守相关的隐私法律与政策。NIST 隐私框架遵循 NIST 网络安全框架（CSF）的结构，促进两个框架的共同使用。与 NIST 网络安全框架一样，隐私框架由三个部分组成：核心层、概要层和实现层。每个部分通过业务和任务驱动因素、组织角色和责任以及隐私保护活动之间的联系来加强隐私风险管理，核心层定义了包括识别、管理、控制、沟通、保护在内的核心功能，用于管理数据处理过程中可能产生的隐私风险。NIST 隐私框架的目的是通过以下方式帮助组织管理隐私风险：在设计和部署影响个人的系统、产品和服务时考虑隐私因素；沟通组织的隐私保护实践；鼓励跨组织员工协作来加强隐私保护。NIST 隐私框架可以帮助组织优化数据的使用以及创新性系统、产品和服务的开发，同时最大限度地减少对个人的不利影响。隐私框架可以帮助组织回答一个基本问题：在开发系统、产品和服务时，应该如何考虑其对个人隐私的影响？

在数字安全治理体系下，所有参与者都需要明确自身的角色与职责；所有安全控制措施则从不同的角度与层面（例如组织层面、人员层面、物理层面、技术层面）提供具体的安全能力与支持，成为数字安全治理最终落地的具体组件，在这个过程中，无论是董事会，管理层，CEO,CIO,CISO,还是每一个组织成员，都在数字安全治理体系下，作为规则制定者、执行者、检查者、遵守者来完成恪尽职守（Due care &Due diligence）。

3.3 数字安全标准

在全球数字经济大力发展的趋势下，全球各国都在积极推动数字经济安全相关标准的研究和编制工作，为数字经济高速发展、安全发展、高质量发展提供了土壤，为强化数字经济安全提供了发展路径和技术指导，为数字经济安全发展指明了方向。

3.3.1 联合国

联合国高度重视数字经济发展和数字经济安全，2022 年 2 月 15 日，联合国开发计划署（UNDP）发布了《2022-2025 年数字战略》，第二部分提出的全社会方法的标准规则中提出了网络安全标准规则，给出了数字安全标准化工作指引。

在这个战略计划中，数字化是帮助联合国开发计划署实现其核心目标的三个主要手段之一。数字技术可以通过促进公民参与和政治参与来推进公平公正，通过认证、数据交换和支付以减少腐败现象。

3.3.2 ITU-T

ITU-T SG17 是 ITU-T 负责制定安全相关标准的工作组。ITU-T SG17 中与数字安全相关的标准项目可分为以下几类：个人信息安全、生物特征信息安全、云计算安全、大数据安全、电子商务与金融科技、生物识别、车联网、区块链等特定行业或技术领域的网络安全。目前，ITU-T SG17 已发布和在研的标准项目包括：X.1033《运营商提供的个人信息服务安全指南》，为运营商开展个人信息服务提供技术指引和实施建议，帮助运营商搭建安全的个人信息服务安全体系、X.1641《云服务客户数据安全指南》，给出了云服务客户数据安全风险指引和防护指”，为云服’客户数据安全以及云服务提供商数据服务安全提供了参考。X.GSBDaaS 《大数据服务安全指南》给出了大数据安全服务的安全要求和实施方案，为供应商提供安全的大数据服务提供参考。X.dlt-sec《使用分布式账本数据进行身份管理中的安全考虑》分析了分布式账本数据面临的安全风险，以及进行身份管理时需要重点关注的安全事项等。

3.3.3 ISO/IEC

ISO/IEC JTC1/SC 27 是 ISO/IEC JTC1 下属信息安全分技术委员会。SC 27 中与数字安全相关的标准可分为以下几类：信息安全管理、ICT 供应链安全、个人信息安全、云计算安全、大数据安全、物联网安全等。其中，ISO27000 标准体系已经成为世界上应用最广泛与典型的信息安全管理标准体系。标准适用于各种性质、各种规模的组织，如政府、银行、电讯、研究机构、外包服务企业、软件服务企业等开展信息安全管理工作。ISO27001

是系列标准的主标准，各类组织可以按照 ISO27001 的要求建立自己的信息安全管理体系(ISMS)，标准体系还包括《ISO 27002 信息技术—安全技术—信息安全管理实践规范》《ISO 27003 信息安全管理体系—实施指南》《ISO 27004 信息安全管理体系—指标与测量》等。《 ISO/IEC 27036 信息技术 安全技术 供应链关系的信息安全》 标准体系由多个标准族集合而成，用于评价和处理供应商在提供服务或产品过程中可能面临的信息安全风险，给出了 IT 产品和服务安全控制的指引，包括《ISO/IEC 27036-1 第 1 部分：概述和相关概念》《ISO/IEC 27036-2 第 2 部分：要求》《ISO/IEC 27036-3 第 3 部分：ICT 供应链安全指南》和《ISO/IEC 27036-4 第 4 部分：云服务安全指南》等。SC 27 中个人信息相关标准有《ISO/IEC 29151:2017 信息技术 安全技术 PII 保护实践指南》等，该标准可供组织在云计算信息安全管理系统实施过程中选择个人信息保护控制措施时参考，也可作为个人信息处理者实施普遍接受的个人信息保护控制措施的指导性文件。SC27 中云计算安全标准有《ISO/IEC 19086-4 云计算 服务水平协议 (SLA)框架 第 4 部分：安全与 PII 保护》等，该标准给出了云服务级别协议（Cloud SLA）个人识别信息组件、SLO 和 SQO 的安全和保护，包括要求和指导。SC27 中大数据相关标准有《ISO/IEC 20547-4 信息技术 大数据参考架构 第 4 部分：安全与隐私保护》等，该标准作为 ISO/IEC 20547 系列标准之一，是 SC27 发布的第一项关于大数据安全与隐私保护的国际标准，标准从用户和功能两个视角对大数据安全与隐私保护的参考框架进行了描述。

3.3.4 NIST

美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）直属美国商务部，从事物理、生物和工程方面的研究，提供标准、标准参考数据及有关服务。NIST 十分重视数字安全相关标准的研制，目前已发布的关于数字安全的相关标准包括 SP 800 标准系列等。SP 800 是美国国家标准与技术研究院发布的一系列关于“信息安全的指南”，在 NIST 标准系列中，虽然 NIST SP 不作为正式法定标准，但在实际工作中，已经成为美国和国际安全广泛认可的事实标准和权威指南。SP800 系列成为了指导美国信息安全管理建设的主要标准和参考资料。SP800-53 作为 NIST 信息安全的支撑性文件，提供了主动且系统的方法，确保关键的系统、组件和服务具有足够的可信度和必要的网络弹性。SP 800-171《非联邦信息系统和组织的受控非机密信息的保护》，保护非法信息系统和组织中的受控未分类信息，NIST SP 800-171 要求是 NIST SP 800-53（FedRAMP 使用的标准）的子集。 NIST SP 800-171 的附录 D 提供了其 CUI 安全要求与 NIST SP 800-53 中相关安全控件的直接映射。SP 800-122《个人可识别信息机密保护指南》给出了个人身份信息保密性方面的保护指南，为安全管理者、安全服务提供商、安全技术开发人员、系统实施人员和系统评估者提供指导。NIST 数字安全相关标准还包括 SP

1800-11《数据完整性：从勒索软件和其他破坏性事件中恢复》等，企业可参照该指南从勒索软件等破坏性恶意软件、内部攻击、员工错误中恢复数据完整性（包括电子邮件、员工记录、财务记录和客户的数据）。

3.3.5 中国信息安全标准化技术委员会（TC260）

中国信息安全标准化技术委员会（TC260）是负责组织开展中国信息安全有关的标准化技术工作的组织。TC260 目前发布的数字安全标准包括：《GB/T 35273-2020 个人信息安全规范》《GB/T 37973-2019 信息安全技术 大数据安全管理指南》《GB/T 35274-2017 信息安全技术 大数据服务安全能力要求》《信息技术 安全技术 公有云中个人信息保护实践指南》等。《GB/T 35273-2020 个人信息安全规范》规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动应遵循的原则和安全要求，适用于规范各类组织的个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。《GB/T 37973-2019 信息安全技术 大数据安全管理指南》提出了大数据安全管理基本原则，规定了大数据安全需求、数据分类分级、大数据活动的安全要求、评估大数据安全风险，标准适用于各类组织进行数据安全管理，可供第三方评估机构参考。《GB/T 35274-2017 信息安全技术 大数据服务安全能力要求》规范了大数据服务提供者的安全能力，包括大数据服务提供者的安全能力，包括大数据服务提供者的基础服务安全能力、覆盖数据生命周期管理的大数据活动安全能力、大数据平台与应用的系统服务安全能力，适用于为政府部门和社会公众提供大数据服务的相关方。

3.3.6 美国国家安全局、美国网络安全和基础设施安全局

2021 年，美国国家安全局发布《企业采用加密域名系统协议的指南》，给出了加密域名系统协议的使用指引，为企业开展相关工作提供了实施路线。《零信任安全指南》给出了部署零信任体系的方法和路线，为零信任安全的部署和工作开展提供了指南。《IT-OT 连接保护指南》分析了 IT-OT 连接保护的安全风险，并针对相关风险给出了具体保护建议。《企业通信系统保护指南》分析了企业通信系统面临的安全风险和风险防范措施。《5G 云安全指南》给出了 5G 云下安全的防护要求和防护建议，为 5G 云安全部署提供了操作步骤。

2021 年，美国网络安全和基础设施安全局发布《防御软件供应链攻击指南》为软件供应链安全提供了保护建议，为动态应对软件供应链攻击提供了实施方案。此外，2021 年度还发布了《针对威胁情报分析 MITRE ATT&CK 指南》《Kubernetes 安全指南》《企业移动设备保护指南》《关于 VPN 的选择和保护指南》等标准。

3.3.7 新加坡

新加坡针对云计算安全领域，提出的多层云安全性标准 SS 584：2020 (MTCS)在国际范围内得到了很大的认可和应用，是全球首个涉及多层云安全性的云安全标准。制定该标准的目的是鼓励采用强有力的云计算风险管理和安全实践，同时提高 CSP 的安全能力，标准中尤其以“数据治理”为控制域，提出了完整的安全措施要求。

2019 年新加坡发布世界上第一部关于高级别自动驾驶汽车应用的国家准则——《自动驾驶汽车技术参考准则（Autonomous Vehicles Technical Reference，TR68）》，为自动驾驶汽车生产企业和技术开发商提供了指导规范，其中第 4 部分规范了自动驾驶车辆数据类型和格式要求。

3.3.8 其他

在国际范围内，更多的国家和地区出于主动捍卫本国数据资源安全、积极融入数字经济新秩序等目的，出台和完善各自的数字安全标准规范。例如：

2021 年 2 月，欧洲网络与信息安全局发布《医疗保健服务云安全指南》

2021 年 11 月，英国政府发布《技术收购安全规则指南》

为了全球数字经济的健康发展，为了人类共同的数字化未来，国际范围内需要能广泛适用和认可的数字安全标准和实践。

第四章 数字安全执行层

数字安全执行层涵盖了规则层落地所需的一切资源/工具及使用这些资源/工具的具体行动，主要包括数字安全技术、数字安全方案/产品、数字安全服务、数字安全教育等内容。

4.1 数字安全技术

4.1.1 原生安全

原生安全是下一代互联网原生安全，包括云计算、大数据、AI、5G/6G、IoT、区块链、量子计算等新兴技术的安全防护措施。

4.1.1.1 云计算

云计算安全技术包括云访问安全代理（CASB）、托管检测和响应（MDR）、软件定义边界（SDP）、基于身份的隔离、容器安全技术等具有显著云安全特性的技术。

- CASB：主要以“安全即服务”(SaaS)模型在云服务本身部署，管理层可以通过 CASB 知悉组织使用的云服务是否安全，查看从一个云传输到另一个云以及在内部部署的基础结构和云之间传输的数据，通过数据加密或混淆、身份验证和访问控制的特定要求等确保数据以安全的方式存储，还可以提供威胁防护，加强云上数据应用的访问和身份验证控制措施。
- MDR：MDR 是一项网络安全服务，根据《全球与中国托管检测和响应（MDR）服务市场现状及未来发展趋势》的研究，MDR 结合了技术和人类专业知识执行威胁搜寻、监控和响应。MDR 的主要好处是有助于快速识别和限制威胁的影响而无需额外的人员配置。
- 零信任：包含 SDP、基于身份的隔离以及 IAM。根据《SDP 标准规范》的研究，SDP 将服务与不安全的网络隔离开来，仅在设备验证和身份验证后才允许访问企业应用基础架构。基于身份的隔离是从软件定义的隔离、微隔离 SEM（微分段）演变而来，基于身份的隔离面向身份定义网络，用于云计算的细粒度的安全访问控制。IAM 是数字身份的核心。
- 云原生安全：根据《云原生安全技术规范》，云原生安全包括容器基础设施安全、容器编排平台安全、微服务安全、服务网格安全、无服务器计算安全。相关技术细分为镜像漏洞扫描、漏洞修复、容器级网络隔离、容器入侵检测、容器环境基线核查、微服务 API 安全防护、微服务应用安全防护等。云原生安全为云计算、虚拟化场景下的业务和应用系统提供安全保障。

4.1.1.2 大数据

大数据开发利用涉及以下安全技术：大数据系统安全、大数据服务安全。

大数据系统安全包括在大数据平台下的物理安全（如环境安全、设备安全），还包括网络安全如防火墙、身份认证与管理 IAM，软件定义边界 SDP、微分段 SIM 等。

大数据服务安全包括在大数据平台下的数据安全服务，以数据分类分级、数据溯源、元数据管理为重点，同时数据脱敏，隐私计算，AI 赋能数据安全等数据安全技术也适应于大数据。

- 数据分类分级：根据《工业和信息化领域数据安全管理办法（试行）》（征求意见稿)，数据分类分级根据数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益等造成的危害程度，工业和信息化领域数据分为一般数据、重要数据和核心数据三级。《信息安全技术 网络数据分类分级要求》（征求意见稿）从国家数据安全管理视角，提出数据分类分级框架，如图所示：

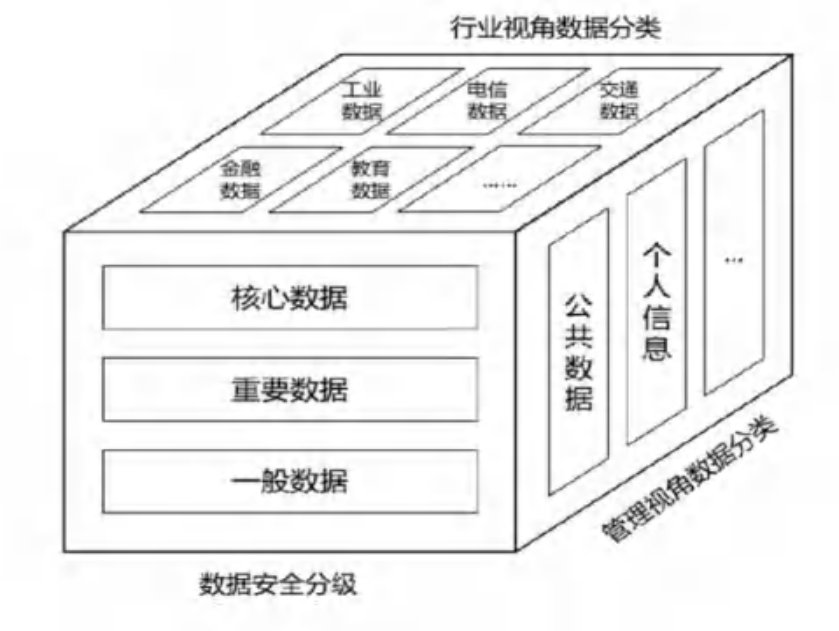


图 4-1 数据分类分级框架

- 数据溯源：数据溯源包括数据标注追踪、数据水印溯源以及基于区块链的溯源等。通过数据溯源能追踪到异常发生的原因，还能帮助人们确定各项数据的来源。

- 元数据管理：在大数据平台中，元数据管理包括数据字典、数据资产清单、血缘分析与追溯系统。数据字典包含数据表和字段名称，含义，类型和长度等基本信息，是偏技术层的元数据；数据资产清单更偏业务，是对应用层的数据资产进行管理的工具；血缘分析，主要是数据的指标和维度的字段，说明数据从哪些实体表逐层传递到最终应用层的数据表。

4.1.1.3 AI

AI 安全既包括样本数据安全，也包括 AI 模型的保护安全。其中，数据安全相关的技术均适应于样本数据的安全。为了保障 AI 整体的安全，AI 模型保护要对抗攻击。AI 模型保护包括 AI 模型本身以及 AI 模型运行环境保护。

- AI 模型自身保护：AI 模型自身保护包括模型提取攻击防御、成员推理攻击防御、模型逆向攻击防御、逃逸攻击防御、后门攻击防御以及数据投毒攻击防御。
- AI 模型运行环境保护：运行环境保护主要涉及端到端加密、存储加密、漏洞扫描与修复、数字签名、访问控制等。

4.1.1.4 5G/6G

5G/6G 网络引入了网络功能虚拟化、网络切片、边缘计算、网络能力开放等关键技术，为大量垂直行业提供服务，因此，网络中将包含大量的用户隐私信息，需要综合多方面技术进行安全保障，这些技术包括设备接入、无线接入、边缘计算、网络切片安全技术等。

- 设备接入：识别允许接入的合规设备，限制违规设备接入，保障网络中信息的通信安全，防止网络窃听等造成数据泄露。
- 无线接入：以密码技术为基础，保护用户数据和信令数据的安全。
- 边缘计算：依据《边缘计算安全技术综述》，边缘计算安全技术主要是密码安全技术，包括基于身份标识的密码技术、RSA 和 ECC 密码技术、基于配对的密码技术、格密码技术、多变量公钥密码技术等，防御设备层、通信层和边缘计算层的安全攻击。
- 网络切片：依据《5G 网络切片安全技术与发展分析》，网络切片安全技术包括切片自身安全、虚拟化安全。切片自身安全技术包括切片隔离、切片接入认证、差异化安全机制、切片通信安全以及用户交互双向认证安全；虚拟化安全包括 VNF 安全、NFVI 安全、MANO 安全等。

4.1.1.5 IoT

依据《物联网安全规范》[13]，物联网安全技术框架如图所示，

[13] https://c-csa.cn/research/results-detail/i-1756/

图 4-2 物联网安全技术架构

物联网系统安全防护主要从物理层、设备层、网络层、应用层展开设计，包括物理安全、设备安全、网络安全、通信安全、无线安全、应用安全以及数据安全。

物联网安全运营和运维主要通过安全事件管理、漏洞管理、日志监控审计、安全配置管理、安全培训、安全操作管理和资产管理来保障。

安全开发主要通过对整个开发流程的安全措施和策略、供应链安全以及安全测试保障安全。

4.1.1.6 区块链

依据国家标准《信息安全技术 区块链技术安全框架》（征求意见稿），区块链涉及的安全技术如图所示：

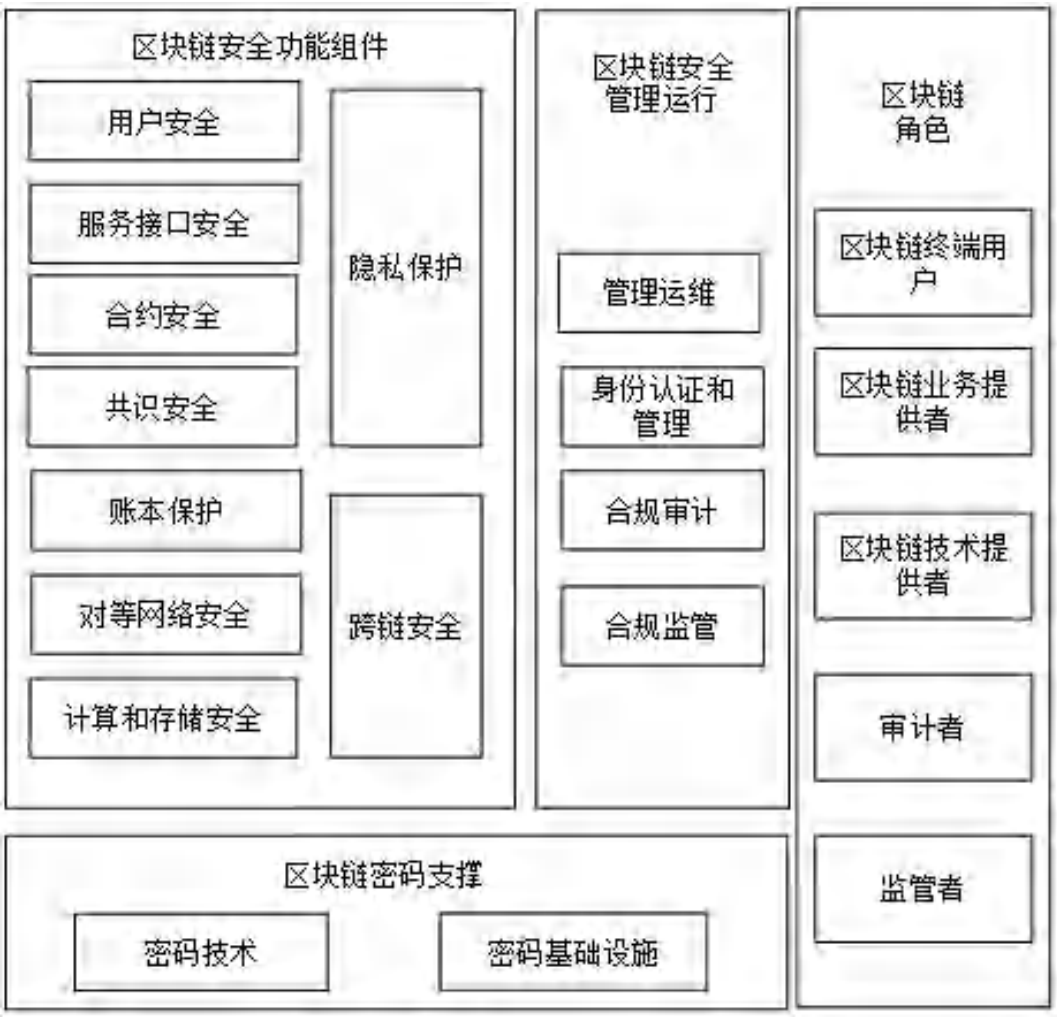


图 4-3 信息安全技术 区块链技术安全框架

- 应用层安全：应用层安全包括 API 接口安全技术以及访问控制技术。
- 合约层安全：合约层安全包括智能合约自身安全技术和智能合约执行环境安全。智能合约自身安全技术，如漏洞安全技术，安全审计技术（规则验证、静态分析、模糊测试技术、形式化验证等技术）；智能合约执行环境安全如沙箱技术、可信追溯技术等。
- 共识层安全：共识层安全包括共识准入，涉及身份认证技术、密码技术等。
- 网络层安全：网络层安全包括白名单或者 PKI 证书机制进行节点准入限制，基于密码技术的通信保密机制以及 DNSSEC 抵御针对 DNS 的中间人攻击。
- 数据层安全：数据层安全包括基于密码技术的隐私保护和保密性、认证授权访问控制技术、数据备份技术。
- 物理环境安全：物理环境安全包括密钥协商、数字信封、密文传输、侧信

道安全技术等硬件相关安全技术。

4.1.1.7 量子计算

量子秘钥分发：量子理界最小的不可再分的基本单位，光的最小单位是光子，即称“光量子”，就是量子的一种，在量子通信中，使用光子的偏振态（光子的相位信息）传递信息。单光子被调制到指定偏振角度，接收端通过一个偏振分波器将光子分束到任一探测器。秘钥分发过程如下：

- 发送端：随机选择 2 组偏振正交基的任意一种调制单光子发送秘钥。
- 接收端：偏振基和发送端相同，即可以准确测量。如果不同，会随机分配到某一个接收器。

经典学的算法和协议大多是基于求解大数质因子分解问题、离散对数问题、二次剩余问题等数学难题的困难性，无法被严格证明是安全的。量子计算机可以在有限的时间内攻破经典密码学中的基于数学难题的算法。

签名阶段，签名方先将源文件进行数字摘要，并用自己的私钥加密该数字摘要构成自己的签名，然后将签名附在源文件后面发送给验证方；验证阶段，验证方收到签名后，先对源文件进行数字摘要，得到数字摘要 1，再用签名方的公钥对签名进行解密，得到数字摘要 2，比较数字摘要 1 和 2，若相等，则签名通过验证，否则签名无效。由此可以看出，数字签名可以提供消息认证、确保消息的完整性并具有不可否认性的功能。

数字签名的实现大多基于公开密钥算法，所以与经典密码学遭遇的困境类似，数字签名方案也容易受到攻破。随着量子密码学的发展，特别是量子密钥分发协议的提出，人们将目光投向了量子领域。

量子数字签名方案结合了量子密码学和数字签名技术，利用量子力学原理可达到无条件安全性。

4.1.2 数字身份

数字身份以 IAM 为代表。依据《IAM 白皮书》[14]，IAM 包括了身份管理、登录认证、访问控制与权限管理、审计与风控。IAM 的架构如图所示。

[14] https://c-csa.cn/research/results-detail/i-1672/

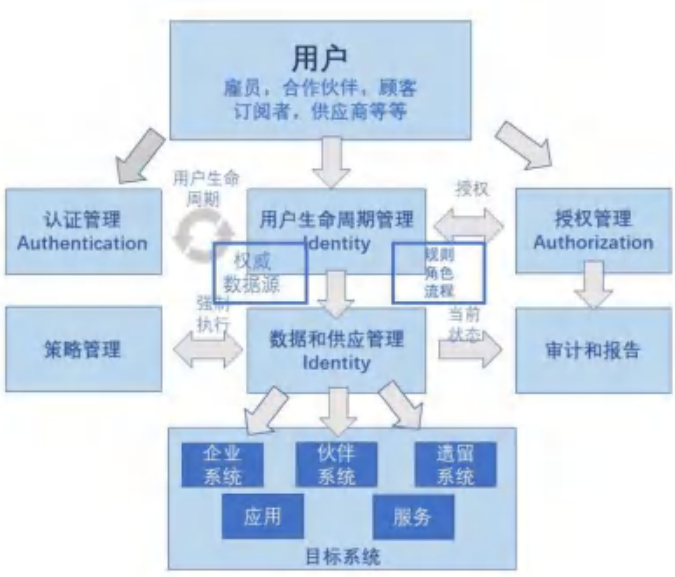


图 4-4 IAM 架构

- 身份管理：旨在构建企业或组织中各类用户在其信息化体系中统一规范的身份识别和管理体系，核心是基于工作流的账号全生命周期管理。身份管理包含用户管理、机构管理、应用管理、数据同步、密码策略管理、生物特征管理以及用户自服务等能力。
- 权限管理：建立权限统一管理的入口，集中管理包含角色、机构、用户组、菜单、按钮等权限。
- 统一认证与访问管理：认证是验证尝试访问受保护资源的实体的凭据的过程，单一登录（SSO）是访问管理的功能，其中用户经过一次身份验证，并且会话的凭据在安全域内的不同应用程序之间判定为可信。统一认证与访问管理提供各类应用的统一登录入口和集中导航，实现一套账号体系登录、全网通行；融合多种认证方式，构建统一认证服务能力。
- 风险管控：事先预设好的风险管理规则，同时根据用户访问元数据（时间、地点、习惯、账号、关系、行为、权限等）实时计算用户访问行为的风险评分，当系统检测到反欺诈风险时，平台主动阻断风险以保证用户访问的安全性。
- 合规审计: 通过平台的可视化报表记录用户访问行为，提供事后追溯能力，同时定期归档审计日志，持久化保存日志数据。

4.1.3 网络安全

网络安全狭义的指网络层的的安全防护与检测技术，广义的是指网络层、应用层、

主机层这三个层次的安全防护与检测技术。

- 网络层安全技术主要包含：DDOS 防护、网络防火墙、网络入侵检测、网络入侵防护、网络漏洞扫描、虚拟专用网（VPN）。
- 应用层安全技术主要包含：Web 应用防火墙、API 安全
- 主机层安全技术主要包含：端点检测与响应、主机漏洞扫描。

4.1.3.1 网络层安全

- DDOS 防护：DDOS 防护手段主要有自主防御方法（如漏洞扫描、补丁更新、过滤服务和端口、检查访客来源等）、高仿服务器防御、高仿 IP 防御、高仿 CDN 防御、配置 WAF 等。
- 网络防火墙：网络防火墙主要有实现技术有以下 5 种：包过滤技术、状态检查技术、应用服务代理、网络地址转换技术、完全内容检测技术。
- 网络入侵检测：网络入侵检测通过镜像流量进行监听分析，并将网络数据包与自身规则库对比，能够及时发现网络的安全现状。目前网络入侵检测主要是通过规则库、行为分析模型进行安全检测。
- 网络入侵防护：入侵防护技术将设备串行到网络中，通过根据流量匹配规则库进行识别，进行阻断和放行，能够识别 2-7 层的网络协议。
- 网络漏洞扫描：漏洞扫描可以划分为 ping 扫描、端口扫描、OS 探测、脆弱点探测、防火墙扫描五种主要技术。按照 TCP/IP 协议簇的结构，ping 采用 ICMP 协议，工作在互联网络层；端口扫描、防火墙探测工作在传输层；0S 探测、脆弱点探测工作在互联网络层、传输层、应用层。
- 虚拟专用网（VPN）：VPN 属于远程访问技术，通过加密技术在不同 Internet 构建虚拟数据通讯隧道，实现数据在此专用虚拟链路上的安全传输。VPN 主要包括 SSL VPN、IPSecVPN。

4.1.3.2 应用层安全

- Web 应用防火墙（WAF）：WAF 检测应用层协议数据，通过分析并匹配规则库确定是否存在威胁访问，判断是阻断还是放行，用于保护应用系统抵御来自应用层的攻击。WAF 主要采用正则表达式，标签器、行为分析、信誉分析以及机器学习等检测技术，一般可以防护 CC 攻击、IP 黑名单、添加安全标头、添加 cookie 的 http-only 标志、实现 HSTS 机制、CSRF 令牌以及

JavaScript 客户端模块等防护检测能力。

- API 安全：API 安全主要以鉴权、认证等访问控制措施进行识别，并校验输入和输出内容。API 安全涵盖基于主机的认证，基本认证，OAuth，OAuth 2.0、SAML。

4.1.3.3 主机层安全

- 端点检测与响应（EDR）：端点检测与响应,采用 agent+服务端架构，在客户端安装 agent，端点将采集的信息上传到服务端并执行策略，服务端负责安全风险分析和策略下发。
- 主机漏洞扫描：主机漏洞扫描技术的实现方式是在目标客户端部署 agent，通过扫描客户端所有系统组件、中间件、数据库以及应用软件的目录和路径、进程等信息，匹配管理端的漏洞库信息，从而判定目标的漏洞状态。主机漏洞扫描技术有两种方式——版本匹配与 POC 验证。

4.1.4 信息安全

依据 ISO 信息安全管理的相关标准，信息安全管理体系 ISMS 是组织整体管理体系的一个部分，是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的体系。

4.1.4.1 质量管理

质量管理包括 PDCA 质量管理模型。PDCA 过程方法也被称为戴明环，是管理学中常用的一个过程模型，该模型在应用时，按照 P-D-C-A 的顺序依次进行，一次完整的 P-D-C-A 可以看成组织在管理上的一个周期，每经过一次 P-D-C-A 循环，组织的管理体系都会得到一定程度的完善，同时进入下一个更高级的管理周期，通过连续不断的 P-D-C-A 循环，组织的管理体系能够得到持续改进，管理水平随之不断提升。

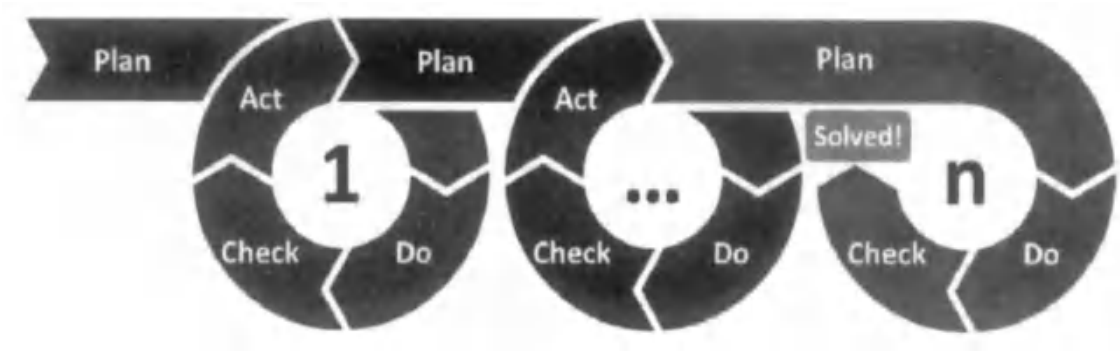


图 4-5 PDCA 质量管理模型

4.1.4.2 商业架构

舍伍德商业架构模型（SABSA）：用于企业安全架构和服务管理的框架和方法论。由于 SABSA 是一个框架，意味着为构建架构提供了一种结构，也就意味着提供了建立和维护架构要遵循的过程。

4.1.4.3 测量模型

信息安全测量模型是将信息相关测量对象与其属性关联的结构。测量对象可包括已计划的或已实施的过程、规程、项目和资源。测量模型如图 4-6 所示，信息安全测量模型描述如何量化相关属性并转换为指标，以提供决策依据。

基本测度是可获得的最简单的测度。基本测度通过对一个测量对象所选择的属性应用测量方法产生。一个测量对象可能有许多属性，但只有部分属性可提供赋予基本测度的有用值。对于不同的基本测度，可使用一个给定的属性。

对每个基本测度应识别其测量方法。测量方法是一种逻辑操作序列，将属性转换为基本测度。测量方法被用于量化测量对象，其操作可能涉及统计出现次数或观测时间推移之类的活动。

一个测量方法能应用于一个测量对象的多个属性。例如，测量对象可以是 ISMS 中已实施的控制措施的执行情况；受控制措施保护的信息资产的状况； ISMS 中已实施的过程的执行情况；已实施的 ISMS 责任人的行为；信息安全责任部门的活动；感兴趣方的满意程度等内容。

一个测量方法可以使用来自不同测量源和属性的测量对象，例如，风险分析和风险评估结果；问卷调查和人员访谈结果；内部和(或)外部审核报告；日志、报告统计和审计轨迹等 事件记录；事件报告，特别是那些产生影响的事件的报告；测试结果，如来自渗透试验、社会工程、符合性测试工具和安全审计等工具的结果；与规程和方案相关的组织信息安全记录，如信息安全意识培训结果。

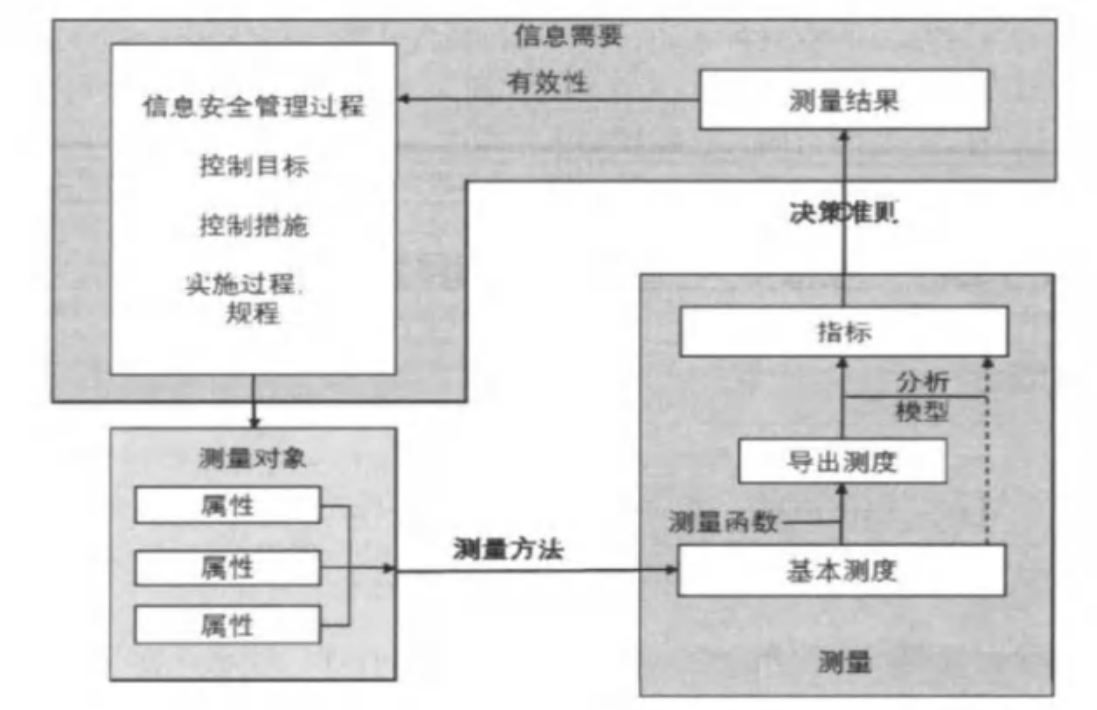


图 4-6 **信息安全测量模型**

4.1.4.4 风险管理

风险管理常见的模型包括 COSO 风险管理模型和 COBIT 风险管理模型。

- COSO 风险管理模型：COSO 建立了一个共同的内部控制模式，公司和组织可以进行评估。
- COBIT 风险管理模型：COBIT 提供了一套可实施的"信息技术控制，并围绕 IT 相关流程和推动因素的逻辑框架组织。

4.1.4.5 能力成熟度

能力成熟度模型 CMM 包括软件工程领域的软件能力成熟度模型(SW-CMM)，传统制造业领域的系统工程能力成熟度模型(SE-CMM)，安全工程领域的系统安全工程能力成熟度模型(SSE-CMM)和系统安全工程能力成熟性模型评估方法(SSAM)等。除此之外，数据安全领域还有的数据安全能力成熟度模型（DSMM），是以 2019-08-30 发布，2020-03-01 实施的 GB/T 37988-2019 《信息安全技术数据安全能力成熟度模型》为依据的数据安全保护体系。

CMM 明确地定义了 5 个不同的"成熟度"等级。一个组织可按一系列小的改进向更高的成熟度等级前进。CMM 为工程的过程能力提供了一个阶梯式的改进框架，基于以

往工程的经验教训，提供了一个基于过程改进的框架图。CMM 还指出一个组织在开发方面需要哪些主要工作，这些工作之间的关系，以及开展工作的先后顺序。一步一步地做好这些工作可帮助组织走向成熟。

4.1.4.6 安全开发

软件安全开发的生命周期包括：

- 生命周期模型(Life Cycle Model)，包括瀑布模型、增量模型、快速原型模型、迭代模型、螺旋模型、净室模型等。
- 综合的轻量级应用安全过程（CLASP），用于构建安全软件的轻量级过程，包括由 30 个特定的活动和辅助资源构成的集合，用于提升整个开发团队的安全意识，并针对这些活动给出了相应的指南、导则和检查列表。
- 软件能力成熟度集成模型（CMMI 模型）：用于评价软件开发组织过程能力成熟度的模型，后来该模型被用于软件开发组织内部的软件过程改进。
- 软件保证成熟度模型（SAMM 模型）：提供了一个开放的框架，用以帮助软件公司制定并实施应对面临来自软件安全的特定风险的策略。
- B81MM (B81 成熟度模型〉：针对多个软件公司的软件安全项目进行研究的模型，该模型量化不同软件安全项目所采取的措施和实践，描述其共性和各自的特点。
- STRIDE 模型：进行威胁建模的实践。
- DevSecOps：在软件开发生命周期的每个阶段自动实施安全措施，支持以敏捷方法和 DevOps 的速度开发安全的软件。DevSecOps 将应用和基础架构安全无缝集成到敏捷和 DevOps 流程和工具中，在软件投入生产环境之前可以更轻松、更快速、以更低的成本加以解决。 此外，DevSecOps 使应用和基础架构安全性成为开发、安全和 IT 运营团队的共同责任，而不仅仅是安全职能的职责， 使软件更安全，可以更快完成开发。

4.1.4.7 业务连续性

- 信息安全事件与应急响应：信息安全事件与应急响应对信息安全事件进行有效管理和响应，最小化事件所造成的损失和负面影响，是组织信息安全战略的一部分。
- 灾难备份与恢复：保证关键业务和应用在经历各种灾难后，仍然能够最大

限度地提供正常服务所进行的一系列系统计划及建设行为，确保关键业务持续运行以及减少非计划宕机时间。灾难备份是灾难恢复的基础，是围绕着灾难恢复所进行的各类备份工作。灾难恢复不仅关注信息系统恢复，而且考虑业务的恢复。

4.1.5 数据安全

数据安全技术包括：数据清洗、数据分类分级、数据访问控制、数据安全审计、数据防丢失、数据加密、数据脱敏、数字版权、数据风险监测评估、数据溯源、数据删除、数据备份、API 数据安全、数据隐私与合规、隐私计算、数据沙箱、零信任下的数据安全、AI 赋能数据安全、人工智能模型、算法安全等。

按照国家标准《信息安全技术 大数据服务安全能力要求》对数据处理活动的划分，数据处理活动分为数据的收集、存储、使用、加工、传输、提供、公开和销毁。

4.1.5.1 数据收集

数据收集安全技术包括数据清洗、数据分类分级、数据隐私与合规等。

- 数据清洗：数据清洗的技术手段主要包括丢弃数据、补全缺失数据、不处理数据、 数据真值转换。
- 数据分类分级:数据分类分级主要是针对数据资产的梳理和管理，也是数据安全防护的基础，在大数据以及数据安全的不同阶段都具有适应性。
- 数据隐私与合规：数据隐私与合规在数据收集阶段需获得收集的授权，尤其是个人信息相关的知情同意。

4.1.5.2 数据存储

数据存储安全技术包括数据访问控制、数据加密、数据防丢失、数据备份等。

- 数据访问控制：数据访问控制主要是针对数据的身份验证与授权。
- 数据加密：以密码学为基础，集中在密钥和算法两方面，遵循密钥管理，应用对称密码算法、 非对称密码算法、密码杂凑算法等保护数据，使用的密码学算法包括国际密码算法的 AES、DES、TDEAh 和国标密码算法 SM1、SM2、SM3、SM4 等。
- 数据防丢失：数据防丢失从网络、终端、邮件对数据进行防泄漏保护，涉及网络协议解析技术、网络包过滤技术、终端监控技术、邮件过滤技术等。

- 数据备份：数据备份包括网络共享和 NAS，磁带备份，基于云的对象备份。数据备份需要配置必要的数据备份、归档与恢复工具，定期对备份和归档数据的可用性、完整性和一致性进行检测。

4.1.5.3 数据使用

数据使用安全技术包括数据访问控制、数据安全审计、数据防丢失、数据加密、数据脱敏、数字版权、数据风险监测评估、数据溯源、 API 数据安全、数据隐私与合规、隐私计算、数据沙箱、零信任下的数据安全、AI 赋能数据安全等。

- 数据脱敏：数据脱敏对结构化、非结构化敏感数据进行处理，比如仿真、数据替换、加密、数据截取、数据混淆等，也包括动态脱敏和静态脱敏。
- 数字版权（DRM）：数字版权包括了加密、数字签名、数字水印、身份认证、加密传输、权限管理等底层技术。
- 数据风险监测评估：对数据使用的环境、上下文等进行风险监测和评估，涵盖了数据分类分级、数据内容识别、人工智能建模等技术。
- 数据沙箱：通过沙箱隔离数据面临的安全风险，保障数据安全。
- 零信任下的数据安全：在风险等级评估的基础上，形成信任等级，对数据使用进行持续的评估和认证，并根据信任等级进行自适应的防护。
- AI 赋能数据安全：在数据安全层面，融合 AI 的技术，应用在数据安全的各个环节。AI 作为底层支撑技术，为数据安全赋能。

4.1.5.4 数据加工

数据加工安全技术包括数据脱敏、隐私计算、AI 赋能数据安全等。

4.1.5.5 数据传输

数据传输安全技术包括数据安全审计、数据防丢失、数据加密、数据风险计策评估、数据溯源等。

4.1.5.6 数据提供

数据提供安全技术包括数据分类分级、数据加密、数据脱敏、数字版权、数据风险监测评估、数据溯源、数据隐私与合规等。

4.1.5.7 数据公开

数据公开安全技术包括数据分类分级、数据脱敏、数据隐私与合规等。

4.1.5.8 数据销毁

数据销毁安全技术包括物理安全中的存储介质销毁和数据安全中的数据删除。

4.1.6 隐私保护

隐私保护包括隐私合规与隐私计算。数据开发利用、价值挖掘、跨境流动等数据生产活动对数据安全和个人信息保护带来挑战，伴随着危害个人隐私、公共利用和国家安全的风险。全球各国都在逐步开展数据安全和隐私保护，相关法律法规渐次出台，对数据生产和数字经济提出了更高的数据合规要求。隐私计算以“数据可用不可见”为指导，在数据不出私域的情况下，通过数据加密、分布式机器学习等技术手段，实现跨域数据协同计算，让数据价值得以释放。

4.1.6.1 隐私合规

中国在 2012 年就开始关注网络数据保护，出台了《规范互联网信息服务市场秩序若干规定》《全国人民代表大会常务委员会关于加强网络信息保护的决定》，明确了“合法、正当、必要”的数据合规原则。2016 年《网络安全法》颁布，2021 年《数据安全法》《个人信息保护法》相继颁布，数据安全与个人信息保护的法律体系成型。在法律法规之外，中国关于信息安全技术的数据处理规范标准更细致地规定了数据采集、传输、应用等数据全生命周期规范，一些标准更细分到专业行业领域。隐私合规成为隐私保护和数据挖掘的重要关注点，也成为大数据产业关联企业机构面临的一项考题。组织需要在保护数据隐私安全的前提下，进行数据流通共享。

4.1.6.2 隐私计算

隐私计算包含人工智能、机器学习、密码学和数据科学等多领域交叉融合的技术体系，能在保护隐私安全和数据不出私域情况下，对数据进行协同计算，实现数据价值最大化，具体涵盖了多方安全计算、联邦学习、同态加密、差分隐私、可信执行环境等技术。

- 安全多方计算：适用于数据量适中但保密性要求较高的重要数据应用；
- 联邦学习：适用于保密性要求不高但数据量大的模型训练；
- 可信执行环境：包括 TEE（可信执行环境）和数据沙箱。性能更优适用于复杂、数据量大的通用场景和通用算法，TEE 安全性受限于硬件的设计与实现。
- 差分隐私：满足差分隐私的数据集能够抵抗任何对隐私数据的攻击，即攻

击者根据获取到的部分数据信息不能推测出全部数据信息，也无法反推出原始数据。

同态加密相比于多方安全计算，在行业上的产品落地相对较难。但在机器学习等一些特定应用场景下，同态加密通过对算法的适配优化，亦能满足实际业务需求。

此外，隐私计算融合应用区块链技术，也逐步成为隐私计算厂商共识，利用区块链的分布式账本、智能合约等技术可以实现参与计算的原始数据链上存证、计算过程关键步骤的上链存证回溯，确保整个计算过程可验证可追溯。

隐私计算技术现状广泛应用于金融、政务和医疗等行业数据要素流通中，助力数据价值安全释放，驱动数字经济发展。

4.1.7 元宇宙安全

保障元宇宙安全是需要综合运用多项技术，同时元宇宙本身的框架也还没有成熟，因此元宇宙安全还在发展中。以下是元宇宙中存在的一些常见安全挑战：

- 身份。 元宇宙用户的身份可以被欺骗，帐户可以被黑客入侵，头像可以被接管。为了应对这些攻击，开发人员必须实施强大的身份安全控制，例如多因素身份验证、加强的身份验证和访问控制。 用户需要小心保护元宇宙应用程序中使用的非托管钱包中的密码和私钥。
- 设备漏洞。 VR 和 AR 眼镜配备大量软件和内存，也是黑客攻击的目标。此外，位置欺骗和设备操纵使犯罪者能够接管用户的身份并在进入虚拟世界后造成严重破坏。为了应对这种攻击，用户需要经常更新 VR/AR 固件。 开发人员需要确保固件在固件公开发布之前经过全面测试和审核。
- 用户间的通信。因为元宇宙体验是为了促进用户间的交流。参与者中的坏人会造成巨大的伤害。 大规模协调至关重要，一种可能性是使用链上智能合约审核逻辑并协调争议解决。
- 数据真实性。 位置、商品质量、评论、用户信息和第三方可信数据都以准确性为基础。 确保数据的真实性可能很困难。使用 TEE（可信执行环境）和区块链技术可以减轻或减轻数据真实性风险。
- 隐私。现在还没有元宇宙相关法规，为真正个性化的沉浸式体验而收集数据的需求存在隐私风险。用户通常不知道他们提供的数据级别，而且虚拟体验没有国界，因此，确保隐私权由平台所有者和开发者决定。使用隐私

保护计算是解决此问题的一种方法。

4.2 数字安全方案/产品

4.2.1 数字安全方案

4.2.1.1 网络安全

网络安全方案通常综合运用以下应用技术：数据包过滤技术、网络地址转换技术、代理服务技术、反向代理技术、状态检测技术、多协议标签交换（MPLS）、沙箱技术、加密算法/加密技术、哈希运算、流量还原、BGP FLOW SPEC、隧道技术、QoS 技术。

图 4-7 网络安全技术方案概览

4.2.1.1.1 网络层安全

网络层安全是数字安全方案中的重要一环，主要包括的内容有：安全边界防护、流量安全检测、邮件安全、安全传输、安全审计等。

（1） 安全边界防护

对安全区域边界中边界防护的实施过程中，应保证跨越边界的访问和数据流通过边界设备提供的受控接口通信；应能够对非授权设备私自联到内部网络的行为进行检查或限制；应能够对内部用户非授权联到外部网络的行为进行检查或限制；应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

- 网络架构：应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；应避免将重要网络区域部署在网络边界处，重要网络区域和其他网络区域之间应采取可靠的技术隔离手段；

- 访问控制：应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；应能根据会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；应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
- 入侵防范：应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

（2） 流量安全检测

流量安全分析是基于网络全流量分析技术，旁路采集、分析和存储所有网络流量，通过威胁情报系统检测已知威胁，通过回溯分析数据包特征、异常网络行为，发现潜伏已久的高级未知攻击。

对安全网络中流量监测的实施过程中，应全面感知网络威胁，实时地识别网络流量数据；及时止损与快速响应，通过安全事件关联分析；完整记录原始流量数据，通过旁路镜像采集并存储网络全部流量；线索追踪与取证，实现从线索挖掘到整个攻击过程的完整复盘；回溯分析与数据挖掘，实现海量数据的快速回溯分析；可疑事件定性分析，真实还原黑客入侵的全过程；异常行为检测，不断增强未知威胁的检测及响应能力；攻击阻断防御，网络异常行为阻断。

（3） 邮件安全

随着计算机技术的高速发展及因特网的广泛普及，电子邮件越来越多地应用于社会生产、生活、学习的各个方面，发挥着举足轻重的作用。人们在享受电子邮件带来便利、快捷的同时，又必须而对因特网的开放性、计算机软件漏洞等所带来的电子邮件安全问题，如:攻击者获取或篡改邮件、病毒邮件、垃圾邮件、邮件炸弹等都严重危及电子邮件的正常使用，甚至对计算机及网络造成严重的破坏。

防范措施有如下几种：对电子邮件子邮件进行加密、采用防火墙技术、及时升级病毒库、识别邮件病毒、启用实时监控防火墙。

（4） 安全传输

密码技术：应采用密码技术保证通信过程中数据的完整性，以确保传送或接收的通信数据不发生篡改、删除、插入等情况。在通信双方建立连接之前，应利用密码技术进行会话初始化验证；通信加密：应对通信过程中的整个报文或会话过程进行加密；加密技术和强度：应采用国家信息安全机构认可的加密技术和加密强度，并最低达到 SSL 协议 128 位的加密强度；数字加密技术使用：应使用数字加密技术（如数字证书方式）进行严格的数据加密处理防止数据被篡改。

对安全通信网络中通信传输的实施过程中，应采用校验技术或密码技术保证通信过程中数据的完整性；应采用密码技术保证通信过程中数据的保密性。

（5） 安全审计

对安全区域边界中安全审计的实施过程中，应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

对安全计算环境中安全审计的实施过程中，应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。应对审计进程进行保护，防止未经授权的中断。

4.2.1.1.2 应用层安全

应用层安全防护主要是指保护应用软件的安全性。组织在开发应用软件时，应注意设计相应的安全功能。

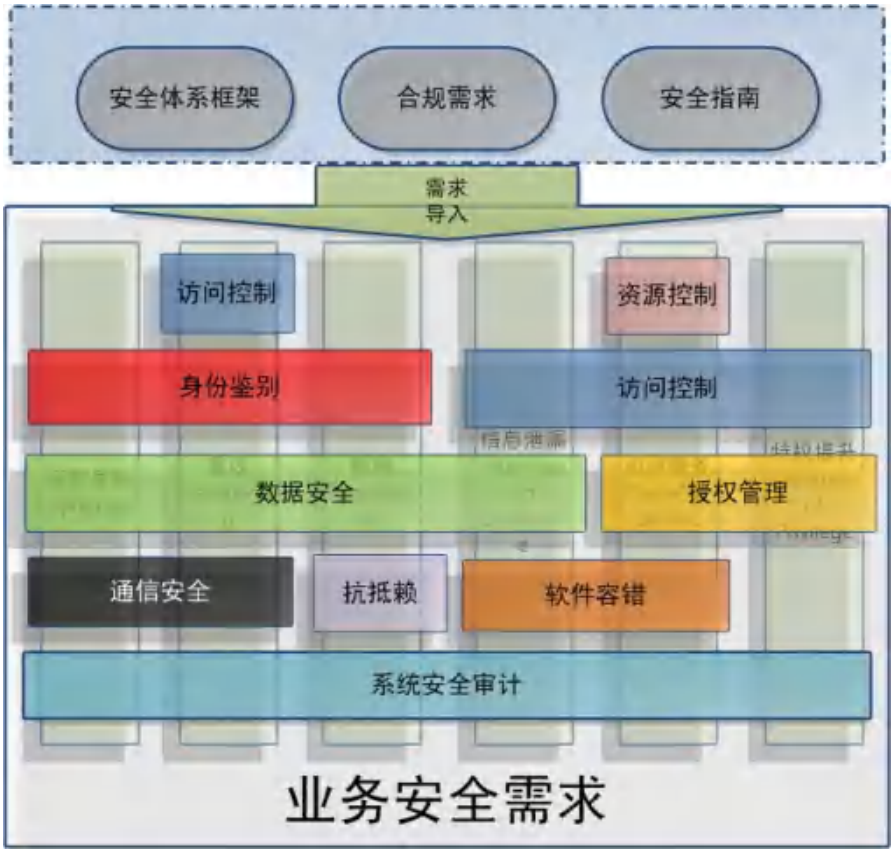


图 4-8 业务安全需求框架图

（1）身份鉴别

- 标识和鉴别：应支持用户标识和用户鉴别；在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；
- 鉴别机制：在每次用户登录和重新连接系统时，采用受安全管理中心控制的口令、基于生物特征的数据、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，且其中一种鉴别技术产生的鉴别数据是不可伪造的，其中如采用密码作为鉴别手段，可考虑主动提供密码长度、复杂度、定期修改以及失败登录次数限定等密码健壮度增强措施。执行重要操作可考虑提供进一步的口令确认；
- 鉴别数据保护：对鉴别数据进行保密性和完整性保护。

（2）授权管理

- 访问授权：应用软件应提供基于菜单、查询功能、报表功能的访问授权；
- 授权清单：应用软件应能自动生成访问授权清单，以方便应用管理员对账

户和其访问授权清单进行检查或清理。

（3）访问控制

- 自主访问控制：应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限部分或全部授予其他用户；
- 控制粒度：应确定自主访问控制主体和客体的粒度，如主体的粒度可以为用户级，客体的粒度为文件或数据库表级和（或）记录或字段级；
- 特权管理：各种访问操作应尽可能使用执行该过程所需的最小用户权限。

（4）抗抵赖

- 数据原发证据：应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；
- 数据接收证据：应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

（5）软件容错

- 输入验证：应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- 自动保护：应提供自动保护功能，当故障发生时自动保护当前所有状态；
- 自动恢复：应提供自动恢复功能，当故障发生时立即自动启动新的进程，恢复原来的工作状态。

（6）资源控制

- 空闲会话限制：当应用系统中的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话，防止维持长时间不活动的会话；
- 会话限制：应能够对系统的最大并发会话连接数进行限制；应能够对单个帐户的多重并发会话进行限制；应能够对一个时间段内可能的并发会话连接数进行限制；
- 资源配额：应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；应能够对系统服务水平降低到预先规定的最小值进行检测和报警；应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。

4.2.1.1.3 主机层安全

建议在外联边界区部署入侵防御系统。

入侵防御系统功能作用如下：对经过外联边界区的病毒、木马、蠕虫、僵尸网络、缓冲区溢出攻击、DDoS、扫描探测、欺骗劫持、SQL 注入、XSS、网站挂马、异常流量等恶性攻击行为进行准确高效的检测并防护。

对安全区域边界中恶意代码的实施过程中，应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

建议在外联边界区边界部署防病毒网关。

防病毒网关功能作用如下：在最接近病毒发生源安全边界处进行集中恶意代码防范，对夹杂在网络交换数据中的各类网络病毒进行过滤，可以对网络病毒、蠕虫、混合攻击、端口扫描、间谍软件、P2P 软件带宽滥用等各种广义病毒进行全面的拦截。阻止病毒通过网络的快速扩散，将经网络传播的病毒阻挡在外，可以有效防止病毒从其他区域传播到内部其他安全域中，截断病毒通过网络传播的途径，净化网络流量，实时查杀网络流量中的各种病毒。

对安全计算环境中入侵防范的实施过程中，应遵循最小安装的原则，仅安装需要的组件和应用程序；应关闭不需要的系统服务、默认共享和高危端口；应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

建议在安全管理区部署 1 台漏洞扫描系统，通过漏洞扫描系统对网络设备、服务器、应用系统等设备的扫描，网络管理员能及时发现安全漏洞，客观评估网络风险等级。网络管理员能根据扫描的结果更正网络安全漏洞和系统中的错误设置，在黑客攻击前进行防范，能有效避免黑客攻击行为，做到防患于未然。

对安全计算环境中恶意代码的实施过程中，应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

4.2.1.1.4 综合类安全

对安全管理中心中系统管理的实施过程中，应对系统管理员进行身份鉴别，只允许系统管理员通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；应

通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

建议在安全管理区部署运维审计系统（堡垒机），运维审计系统可以对内部运维人员的操作进行有效的管控，帮助用户统一管理与运维操作相关的帐号、密码、访问控制、权限控制、审计等一系列行为。它着眼于解决关键 IT 基础设施的运维安全问题。能够对 Unix、Linux、Windows 主机、服务器以及网络设备上的数据访问进行安全、有效的操作审计，支持实时监控和事后回放。可以弥补传统审计系统的不足，将运维审计由事件审计提升为操作审计，集身份认证、授权、审计为一体，有效地实现了事前预防，事中控制和事后审计。

运维审计系统功能包括：

- 身份认证及授权管理。通过对帐号整个生命周期的监控和管理，及时发现帐号中存在的安全隐患，并且制定统一的、标准的用户帐号安全策略；
- 运维事件事中控制。针对运维过程中可能存在的潜在操作风险，根据用户配置的安全策略，对违规操作提供实时告警和阻断，从而达到降低操作风险及提高安全管理与控制的能力。
- 运维事件事后审计。运维审计系统能够对日常所见到的运维协议会话过程进行完整的记录，以满足日后审计的需求。

对安全管理中心中审计管理的实施过程中，应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

对安全管理中心中安全管理的实施过程中，必须要符合以下技术要求：应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

对安全管理中心中集中管理的实施过程中，应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；应对安全策略、恶意代码、补丁升级等安

全相关事项进行集中管理；应能对网络中发生的各类安全事件进行识别、报警和分析。

4.2.1.2 信息安全

信息安全是指保护信息在系统和网络中的传输、处理和存储过程中不被破坏或泄露，确保信息的可用性、机密性、完整性和不可否认性。

可用性（Availability）是指授权主体在系统服务运行时能访问到信息的能力。可用性是在信息安全保护阶段对信息安全提出的新要求，也是在网络化空间中必须满足的一项信息安全要求。

机密性（Confidentiality）是指对数据的访问限制，只有被授权的人才能使用。

完整性（Integrity）是指保证数据在未经授权的情况下不被改变或删除。完整性的目标一是阻止未授权的人有能力修改数据，二是提供一种将数据恢复到一个已知状态的手段。

不可否认性（Non-repudiation）又称抗抵赖性，是指信息交换的双方不可否认交换过程中所发送或接收到信息的行为。不可否认性一般与身份的真实性结合，通过对主体的授权控制实现信息安全目标。

信息安全方案通常综合运用以下应用技术：数据包过滤技术、关联分析技术、沙箱技术、网络欺骗、SOAR、UEBA、AI/ML/DL、数字签名、SDP（软件定义边界）、MSG（微隔离）、IAM（身份权限管理）、规则库/样本库、脱壳技术、非对称加密、对称加密、反向代理、告警降噪算法、数据采集、数据抽取、数据清洗、数据存储、数据挖掘、加密算法、哈希运算、回归算法、分类算法、聚合算法、序列算法、数据可视化。

图 4-8 信息安全技术方案概览

4.2.1.2.3. 安全战略

信息安全涉及保护所有形式的信息，安全战略用来定义所有的架构和策略，并以此构成一套防御、检测和威慑的综合安全体系。企业应根据自身的发展目标制定安全战略，设置合理的安全预算，明确安全愿景和安全目标，组建安全团队，并设计中长期安全规划建设任务、实施路径和重大任务群。

安全战略的基本内容应包含安全职责和授权、安全建设体系计划、安全风险评估及策略制定、安全措施的时间规划、安全实施及维护等。

其中安全建设体系是战略的核心组件，包括安全管理体系、安全技术体系、安全运营体系、安全合规体系等。企业根据自身的安全建设体系，可以从资产、漏洞、威胁、事件等维度开展体系化、立体化、全方位的安全风险管理，定期开展安全效果度量、安全操作审计等工作，迭代提升安全运营效能。

4.2.1.2.1.安全运维/运营管理

安全运维体系通常由人员组织、安全策略制定、安全运维制度和相关技术手段等组成。可通过平台化的安全运维方案提供更有效的运维管理。安全运维平台一般可提供漏洞管理、资产测绘与资产管理、攻击面管理、威胁情报、安全运维审计（堡垒机）、安全基线与配置管理、入侵与模拟攻击、SOAR（安排编排与自动化响应平台）、安全应急响应工具、密码管理、网络攻防指挥平台、网站监测平台等。

4.2.1.2.2. 安全合规方案

等保一体机是遵循国标 GB/T 22239《信息安全技术信息系统安全等级保护基本要求》的要求，对等保二三四级信息系统进行自查评估和整改加固的信息系统。从物理安全、网络安全、主机安全、应用安全、数据安全等多个层面进行体系化的建设和运维。同时，通过等保一体机提供的定制化安全增值服务，实现全网动态监测、精确感知、主动防护。

相较等保一体机，等保检查工具箱侧重于对信息系统进行等保评估检查，为等保安全整改和监督检查提供技术支撑。

密评检查一体机是较新的一类合规方案，类似与等保一体机的定位，遵循 GB/T 39786《信息安全技术 信息系统密码应用基本要求》，针对信息系统的商用密码应用安全性测评工作提供测评过程辅助和测评过程管理，内部集成了多款密码学测评工具，一般包括密码算法检测、通信协议检测、数学证书检测、随机数检测等检测工具。

4.2.1.3 数据安全

图 4-9 数据安全技术方案概览

4.2.1.3.1.数据安全治理类

数据安全方案通常综合运用以下应用技术：网络嗅探技术、正则匹配、NLP 自然语言处理、机器学习、特征工程技术、自动聚类算法。

基于标签的数据分类分级方案：

（1）数据自动发现

基于网络嗅探技术，可自动寻找发现网络环境中存在的海量数据和锁定保护对象，在指定 IP 地址范围内，通过端口扫描自动化发现网络环境中存在的数据库系统。

（2）数据分类分级模板定制

根据行业细分如金融、证券、电信等；根据法律法规细分如网络安全法、GDPR、个人信息安全规范、等保等。用户可根据行业特性以及业务场景选择合适的分类分级模板开展数据分类分级工作。

（3）数据自动化分类分级

如基于深度学习+条件随机场的命名实体识别模型，准确、高效的识别中英文姓名、地址、机构名称等；基于 NLP 技术的文本识别模型、判断敏感文本数据、如：合同、简历、病例等；基于传统的正则表达式、字典等识别规则进行敏感数据识别。

（4）敏感数据可视化

数据安全分类分级监管大屏展示，通过可视化视图全面掌握用户数据库、存储系统，从数据维度获取数据资产情况，有效监控敏感数据流转路径和动态流向。

（5）数据资产目录

支持数据源，敏感数据和所选定的分级标准等多维度进行展示。支持分级概览，表列分布，级别分布等情况图标展示及详情展示，方便使用者了解数据资产的分布情况，同时提供对敏感列识别规则及分类分级信息修改功能。

4.2.1.3.2. 数据安全监测预警类

数据安全监测预警方案使用如下应用技术：数据库审计、漏洞检测、用户行为分析、弱点检测、流量数据监控保护审计、数据自动聚合检测、弱点检测、数据库风险评估、数据库账号使用风险检测。

（1）数据库安全检测预警方案

通过对数据库数据发现梳理及访问行为进行实时监控，经过相关告警规则的识别分析，得出数据库访问风险，并进行预警。

（2）实体与用于行为分析方案

对接入流量日志通过内置算法特征计算，得出实体与用户行为风险，并且 AI 算法有学习能力，能自动识别已学习风险。通过多维度对数据安全风险进行展示分析，形成数据安全态势感知。

4.2.1.3.3. 数据安全防护类

数据安全防护方案使用如下应用技术：敏感数据识别、静态数据脱敏、动态数据脱敏、数据加密、正则匹配、API 安全、细粒度访问控制、流程审批控制、虚拟补丁、身份鉴别、可信执行环境、安全多方计算、联邦学习、零信任、容器安全、云访问安全代理（CASB）、水印（屏幕水印、文档水印、打印水印、隐写水印等）、溯源追踪、文件外发防护预警、数据与文件使用策略。

（1）数据脱敏方案

通过数据静态脱敏的方法，对数据进行敏感数据转化，在不改变原有数据的特征情况下，可以对数据进行外发、分析、测试等操作；通过数据动态脱敏，防止用户访问直接查询敏感信息，造成数据泄漏。

（2）特权用户访问解决方案

对用户进行统一访问管理，建立完善的用户访问防护制度，通过敏感数据发现、动态脱敏、数据库协议解析、SQL 语法解析和改写、脱敏算法、细粒度访问控制、风险操作审批、身份鉴别等能力，对特权用户进行访问控制。

（3）漏洞攻击解决方案

通过对数据库或者系统的漏洞风险识别，分析漏洞危害等级，并提供相应的修复建议及能力。这些能力包括：攻击特征识别、虚拟补丁、细粒度访问控制、会话阻断/拦截等。

（4）敏感文件外发解决方案

通过敏感文件信息识别、外发管控、屏幕水印、文档水印、打印水印、隐写水印、溯源追踪等能力，对实际使用文件终端，进行统一策略控制，赋予实际使用权限，防止文件外发造成数据泄漏等风险。

4.2.1.3.4. 数据安全审计类

数据安全审计方案使用如下应用技术：数据库审计、区块链审计、审计报表、风险告警、敏感数据策略响应、三层关联、风险捕捉、Agent 可控可管、AC 算法、加密审计、访问控制及审批。

数据库访问与审计方案通过对数据库数据识别及访问流量审计，以全面审计和精确审计为基础，实时记录数据库活动情况，对数据库操作进行细颗粒度审计的合规管理，进而对数据库遭受到风险行为进行实时告警。并且对访问行为进行访问控制与审批，阻断危险操作行为。

4.2.1.3.5. 数据安全合规类

数据安全合规方案使用如下应用技术：数据库审计、区块链审计、审计报表、风险告警、敏感数据策略响应、三层关联、风险捕捉、Agent 可控可管、AC 算法、加密审计、访问控制及审批。

（1）数据库访问与审计方案

通过对数据库数据识别及访问流量审计，以全面审计和精确审计为基础，实时记录数据库活动情况，对数据库操作进行细颗粒度审计的合规管理，进而对数据库遭受到风险行为进行实时告警。并且对访问行为进行访问控制与审批，阻断危险操作行为。

（2）数据合规检测及风险解决方案

移动应用合规平台、数据安全合规检测系统

4.2.1.3.6 数据安全综合平台类

数据安全综合平台方案使用如下应用技术：组件统一管控、策略统一下发、数据统一收集、组件状态实时监管、数据安全态势感知、接口全面标准 API 化、数据安全风险

检测预警、数据风险流转溯源。

数据安全统一管控方案通过数据安全管理平台对整体数据安全能力做统一管理工作，具体管理内容：数据安全态势感知、安全组件统一管控、策略统一下发、风险数据统一收集、风险分析、风险展示、事件处理、工单处理、数据溯源。

4.2.1.3.7 数字证书安全

- 数字证书：摘要算法、数据指纹、非对称加密算法、摘要算法。
- 数字签名：签名检查、签名校验、证书签名、证书链、时间戳、信息摘要、证书校验、hash。
- 标识和鉴别：应支持用户标识和用户鉴别；在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性。
- 鉴别机制：在每次用户登录和重新连接系统时，采用受安全管理中心控制的口令、基于生物特征的数据、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，且其中一种鉴别技术产生的鉴别数据是不可伪造的，其中如采用密码作为鉴别手段，可考虑主动提供密码长度、复杂度、定期修改以及失败登录次数限定等密码健壮度增强措施。投资者发出申购、赎回等重要操作，可考虑提供进一步的口令确认。
- 鉴别数据保护：对鉴别数据进行保密性和完整性保护。

4.2.1.4 隐私保护

图 4-10 隐私保护技术方案概览

4.2.1.4.1 隐私计算类

隐私计算方案使用如下应用技术：隐私增强计算技术（PEC）、差分隐私、同态加密、安全多方计算（MPC）、零知识证明、私有集合交集、AI 技术、安全计算沙箱、联邦学习与预测、区块链、区块链溯源技术、ID 融合、同态构型。

（1）隐私计算方案

（a）隐私计算智能服务平台

保证原始数据不出本地即可完成多方数据联合建模和联合计算能力，同时支持安全隐私保护集合、安全隐私查询、安全统计分析。实现各合作机构数据在流通、计算过程中，端到端的安全保护和可审计。

（b）隐私计算一体机

提供一站式隐私保护计算解决方案，具有自主可控、安全可证、隐私保护等特点，实现开箱即用，助力实现数据流动与共享，降低隐私计算开发门槛

（c）隐私计算应用 OS

提供数据隐私保护与数据合规应用能力。提供内核层、服务层、应用层的隐私计算能力输出，全方位覆盖数据应用层次。

（2）隐私数据安全解决方案

行业隐私保护智能解决方案在包括同态加密，秘密分享，不经意传输等基础之上，做了隐私保护计算应用层的中间层框架，使用多方安全计算支持的联合统计，隐私集合求交，匿踪查询功能。还有一部分是和区块链结合，保障云端对于隐私数据的授权和使用的过程，是留痕的、可溯源可审计的，提高隐私合规能力。

4..2.1.4.2 隐私合规类

隐私合规方案使用如下应用技术：AI 检测、区块链、隐私计算、多方安全计算、联邦学习、行为合规检测、权限合规检测、第三方 SDK 合规检测、隐私保护算法引擎、数据管理引擎。

（1）隐私合规平台/隐私合规检测/隐私影响评估

（a）隐私合规评估检测平台

提供隐私风险项检测、隐私专项检测、场景检测、权限过度收集与使用情况检 测等

产品服务，深度挖掘 App 隐私合规风险产生的源头

（b）APP 隐私合规检测工具

行业 App 隐私合规检测、权限合规检测、第三方 SDK 合规检测等

（c）隐私合规管理平台

全生命周期的个人信息管理平台，能够解决企业和机构在收集、存储、使用、分享等个人信息处理过程中遇到的合法合规风险和问题，平台以遵从个人信息相关法律法规为基础，针对企业和机构的合法诉求，提供完善且具有竞争力的产品和解决方案，帮助企业规避合规风险，实现数据价值的最大化。

（2）数据隐私协作平台方案

（a）隐私数据发现及分类

发现并盘点个人信息，提供数据在组织中驻存、流动的可视化能力；在基础设施、数据存储及界面上集成隐私保护能力；支持识别、归类和保护个人隐私数据。

（b）流程映射

数据资产发现，同时包括计算节点、存储及相关组件；包括内置的业务流程映射、自动化识别并集成第三方流程。

（c）行为监控

自动化的处理数据流，持续的监控各类隐私数据的处理环节，并对可疑的行为触发告警，能够减少大量人力资源。

（d）任务管理

根据角色、业务类型、业务范围制定任务计划，促进和保障相关人员、业务按照计划执行行动。提供隐私数据保护向导，降低隐私保护任务、操作相关步骤的行动难度。

4.2.1.5 元宇宙安全

保障元宇宙安全是需要综合运用多项技术，涉及原生安全、数据安全、隐私保护，也包括传统的网络安全和信息安全等多个领域。同时，元宇宙本身的框架也还没有成熟，因此元宇宙安全还在发展中，目前市场上还没有专门针对元宇宙安全的特定技术和方案。

4.2.1.6 数字身份领域

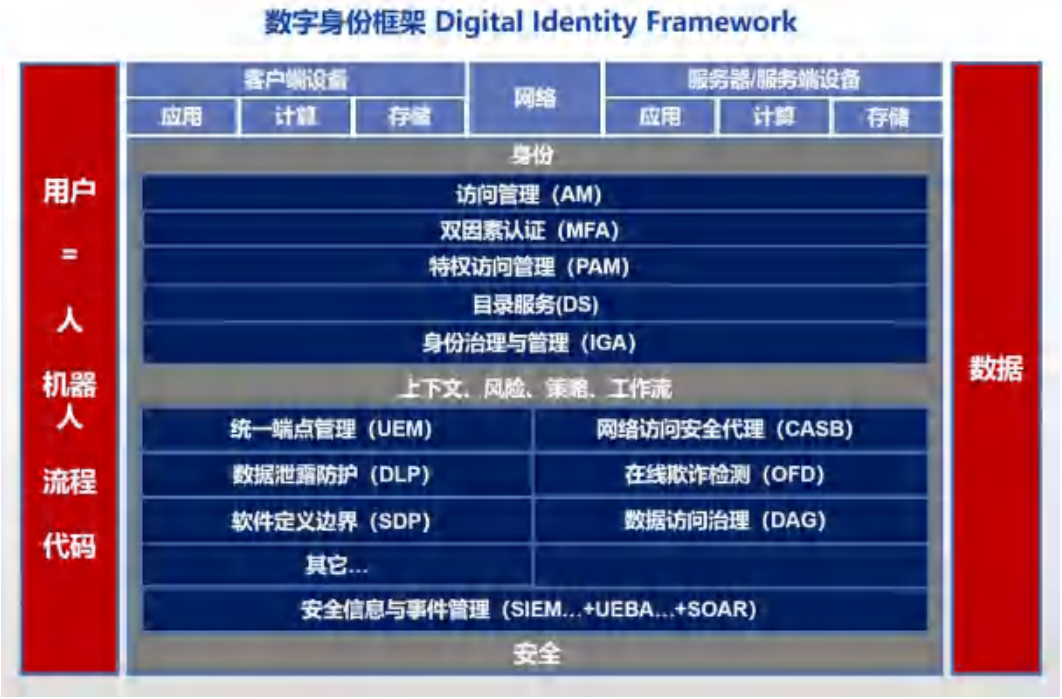


图 4-11 数字身份框架

4.2.1.6.1 数字身份基础支撑类（PKI）

对安全计算环境中身份鉴别的实施过程中，应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

数字身份基础解决方案涉及以下应用技术：PKI 技术、数字证书、认证机构、对称加密、非对称密码技术、密钥备份、证书作废、OCSP 技术（在线证书状态协议）。

（1）CA 统一身份认证解决方案

CA 统一身份认证系统：以 PKI/CA 为基础，通过统一用户管理、统一认证方式、单点登陆、多点漫游、共享的信息服务及安全审计。

（2）统一认证解决方案

统一认证系统：通过用户管理、账号管理、权限管理、审计管理等，实现对人员信息、组织信息、应用信息、账号信息的高效统一管理。

4.2.1.6.2 目录服务类

目录服务解决方案涉及以下应用技术：LDAP 目录服务技术、ADSI 目录服务技术

身份目录解决方案帮助企业实现身份、应用、端的管理。

对目录服务器的访问操作应进行读写分离，同时设计一主多从的服务架构。这样的设计不仅可以优化目录服务器的响应时间，而且还提高了目录服务器的可用性。

4.2.1.6.3 数字身份治理类（身份供应，和 HR 等系统的对接）

数字身份治理解决方案涉及以下应用技术：单点登录 SSO、SCIM\LDAP 协议 CA 身份管理中心、多因素认证 MFA。

数字身份管控平台基于大数据的相关技术的发展、安全数据的共享、对安全事件的联动处置等需求，可采用开放式的安全架构，各类安全设备提供标准化的 API 接口，尤其数据采集类设备（DPI、APT 等）均可与第三方安全分析平台进行数据共享。云安全平台也可提供标准化的对接标准，可接入第三方产品，满足用户的个性化需求。

4.2.1.6.4 数字身份统一认证类（SSO 单点登录、MFA 双因素认证）

数字身份统一认证解决方案涉及以下应用技术：

- MFA 双因素认证技术：动态口令认证、二维码认证、短信认证、生物识别认证、RSA 认证、基于数字证书的身份认证、基于口令的身份认证、OAUTH API 访问授权开放协议。
- SSO 和 MFA 应用技术：SSO 单点登录、cookies 技术、Broker-based、代理认证、 口令认证、基于安全断言标记语言(SAML)实现。

（一）统一身份认证 SSO 平台方案

统一身份认证平台将分散的用户和权限资源进行统一、集中管控，这种模式帮助用户更容易实现单点登录 SSO，简化用户登录多个系统的过程。用户只需要通过一次强身份认证（比如移动端指纹认证和 PC 端扫码登录等），就可以免登录访问授权范围内的所有系统应用，对用户账户的生命周期统一管理。

（二）MFA 双因素认证方案

内置动态口令认证、二维码认证、短信认证、生物认证、RSA 认证等，并对用户访问环境和访问行为进行动态风险评估，基于策略匹配相对应等级的认证方式。

4.2.1.6.5 数字身份权限管理类（IAM 中的权限管理模块）

数字身份权限管理解决方案涉及以下应用技术：基于角色的访问控制（RBAC）、基于属性的访问控制（ABAC）、PIAM 特权用户身份与访问管理、移动安全认证技术、LDAP 协议代理技术、SSH 协议代理技术）。

IAM 权限管理解决方案提供权限管理、访问控制和身份认证的基础服务，您可以使用 IAM 创建和管理用户、用户组，通过授权来允许或拒绝他们对云服务和资源的访问，通过设置安全策略提高帐号和资源的安全性，同时 IAM 为您提供多种安全的访问凭证。

4.2.1.6.6 数字身份审计类（IAM 审计模块）

数字身份权限审计解决方案涉及以下应用技术：认证日志审计、授权日志审计、访问日志审计、用户审计。

统一身份审计管理解决方案提供安全审计（用户身份审计、操作行为审计、高危行为审计、审计查询、审计分析报告）。

4.2.1.6.7 用户异常行为分析类（UEBA）

用户异常行为分析解决方案涉及以下应用技术：大数据分析、机器学习、行为分析、全时空分析、异常检测、基线及群组分析、安全知识图谱、强化学习、特征工程会话重组、身份识别、集成学习风险评分。

UEBA 方案包含自定义机器学习模型、风险优先级告警、用例管理、异常检测、异常行为和观察名单、仪表盘与报告。

UEBA 方案利用 AI 技术实现用户行为分析（UEBA），通过机器学习算法快速训练客户现场安全场景，对异常行为进行定位跟踪，风险阈值实现智能动态调整，实现智能安全判定，对残余风险、隐蔽威胁、未知攻击和 0day 攻击等未知风险进行检测。

4.2.1.6.8 特权访问管理类

特权访问管理解决方案涉及以下应用技术：PAM 特权访问管理、PEDM 特权提升和授权管理、持续发现特权账户、多因子身份验证、会话管理、一次性密码、用户及实体行为分析（UEBA）。

特权访问管理解决方案提供特权访问管理器、云授权管理器、端点特权管理器、供应商特权访问管理器，基于移动安全认证核心技术、LDAP 协议代理技术、SSH 协议代理技术，把特权账号纳入 IAM 统一管理范畴，实现统一安全认证与行为审计功能，实现包括主机操作系统、数据库、中间件、安全设备以及 web 应用涉及的各类特权账号的安全

管理，满足等保合规要求。

4.2.1.6.9 零信任类

零信任解决方案涉及以下应用技术：SDP 软件定义边界、IAM 身份权限管理、微隔离、可信身份代理网关、可信应用代理网关、可信 API 代理网关、可信环境感知系统、手机令牌、零信任控制平台。

零信任综合解决方案通过网络隐身、动态自适应认证、终端动态环境检测、全周期业务准入、智能权限基线、动态访问控制、多源信任评估等核心能力，满足新形势下多业务场景的应用安全访问需求。

4.2.1.7 原生安全

图 4-12 原生安全技术方案概览

4.2.1.7.1 物联网

物联网解决方案涉及以下应用技术：通过各种信息传感器、射频识别技术、全球定位系统、红外感应器、激光扫描器等各种装置与技术，实时采集任何需要监控、 连接、互动的物体或过程，采集其声、光、热、电、力学、化学、生物、位置等各种需要的信息，通过各类可能的网络接入，实现物与物、物与人的泛在连接，实现对物品和过程的智能化感知、识别和管理。

（1）资产高可见方案

通过提供对制造运营各个方面的前所未有可见性，帮助使这些环境成为可能。它们可以监控环境条件，评估生产线的状态，发现问题和潜在的安全威胁，甚至允许技术人员远程控制关键操作。然后，所有这些数据都可以传输到本地微型数据中心或附近的边

缘数据中心，并由强大的分析程序进行处理，从而使制造工厂能够识别趋势并优化操作，以获得更好的性能。

（2）脆弱性管理方案

通过优先处理高风险，使用脆弱性扫描工具针对系统清单来频繁地扫描并识别系统弱点，且尽快处理最高风险的脆弱性。通过修补漏洞来减少攻击面和降低安全风险。

（3）补丁管理方案

通过获得和升级 IOT 设备固件，并且学习正确的 c 语言、Java 和其它源代码级别中的正确代码可以自动生成补丁，以及改变程序的形式而不改变它的功能。

（4）入侵检测方案

分为基于网络的入侵检测系统和基于主机的入侵检测系统。通过监视、分析用户及系统活动，查找非法用户和合法用户的越权操作；审计系统构造和弱点，并提示管理员修补漏洞；统计分析异常行为模式，发现入侵行为的规律；评估重要系统和数据文件的完整性，如计算和比较文件系统的校验和等来实现入侵检测。

（5）数据传输方案

满足大并发物联网设备连接 VPN 的要求，提供后续性能保障；满足数据传输安全，支持国密传输；满足客户端接入节点适配物联网专业系统环境接入需求；支持证书认证、硬件特征码认证等方式，保障合法的客户端才能接入总部系统。

（6）网络隔离方案

在两个或两个以上的计算机或网络在断开连接的基础上，实现信息交换和资源共享。通过将有害的网络安全威胁隔离开，以保障数据信息在可信网络内在进行安全交互。并且以访问控制思想为策略，物理隔离为基础，并定义相关约束和规则来保障网络的安全强度。

4.2.1.7.2 区块链

区块链解决方案涉及以下应用技术：数字货币、金融资产的交易结算、数字政务、存证防伪数据服务等领域。区块链是将数据区块有序链接，每个区块负责记录一个文件数据，并进行加密来确保数据不能够被修改和伪造的数据库技术。

（1）身份和访问管理方案

通过用高度可信的身份和访问管理机制取代传统系统，从而让用户对自己的 ID 有更大的控制权，确保拥有数字身份的人员和实体能进行对企业资源（如网络和数据库）

设置适当访问级别的实践。用户角色和访问权限通过系统进行定义和管理。

（2）密钥管理方案

密钥管理方案是一门综合性的技术，涉及密钥的产生、检验、分发、传递、保管、使用、销毁的全部过程。通过密钥产生器借助于某种噪声源产生具有较好统计分布特性的序列，然后再对这些序列进行各种随机性检验以确保其具有较好的密码特性。好的密钥应当具有良好的随机性和密码特性。

（3）数据保护方案

区块链提供的增强数据安全性是使用区块链作为技术的主要好处。通过加密和验证，确保用户的数据是加密的。以及去中心化的数据保护方式，不依赖于一个中央控制点，而是交易的数字分类账，每台计算机都拥有完整的数据副本。不包含在中心位置，所以区块链没有单点故障，也无法从单台计算机更改。

（4）安全传输方案

在进行区块链数据传输时，需要对数据进行加密，原有的加密方式由于技术老旧、破译容易常常造成数据的缺失，因而采用同态加密的方式进行数据保护，可以在加密的同时对数据进行检测与纠正，保证数据的完整性。

（5）安全合约方案

用计算机语言取代了法律语言记录条款并由程序自动执行的合约。通过传统合约的数字化版本，跑在区块链网络上，由程序自动执行。采用目前可用的最高级别的数据加密，与加密货币使用的加密技术相同。这样使得保护水平在万维网上是最好和最安全的。

（6）安全交易方案

去中心化的分布式账本，改变了原有的交易模式。然而新模式的出现和发展带来了许多交易安全问题，严重威胁用户资产安全。包括攻击、骗局、账户行为、私钥泄露和智能合约漏洞等，通过从交易记录异常检测、地址异常检测、智能合约检测、行为异常检测以及智能合约漏洞检测工具 5 个方面检测区块链交易安全。

4.2.1.7.3 量子计算

量子计算机理论上具有模拟任意自然系统的能力，同时也是发展人工智能的关键。由于量子计算机在并行运算上的强大能力，使它有能力快速完成经典计算机无法完成的计算。这种优势在加密和破译等领域有着巨大的应用。可以应用在天气预报、药物研制、交通调度、保密通信等领域。

（1）量子密码方案

量子密码是基于量子力学机制的信息处理技术，通过量子纠缠来实现经典密钥算法协商，并利用量子纠缠传递经典对称密码密钥。

（2）量子密钥分发方案

利用量子力学特性来保证通信安全性。它使通信的双方能够产生并分享一个随机的、安全的密钥，来加密和解密消息。通过量子叠加态或量子纠缠态来传输信息，通信系统便可以检测是否存在窃听。当窃听低于一定标准，进而产生了一个有安全保障的密钥。

（3）量子数字签名方案

通过签名方先将源文件进行数字摘要，并用自己的私钥加密该数字摘要构成自己的签名，然后将签名附在源文件后面发送给验证方，在验证阶段，验证方收到签名后，先对源文件进行数字摘要，得到数字摘要 1，再用签名方的公钥对签名进行解密，得到数字摘要 2，比较数字摘要 1 和 2，若相等，则签名通过验证，否则签名无效。

4.2.1.7.4 云原生安全

（1）云原生应用安全防护方案

API 安全检测产品、微服务访问控制、微服务漏洞扫描，函数隔离工具、Serverless 资产业务梳理 、平台账号安全防护。

（2）云原生研发过程安全方案

安全威胁建模、静态代码检测、交互式安全测试、动态安全测试、开源组件检测、制品安全、安全配置检测、代码运行监测。

（3）云原生数据安全方案

数据加密、数据备份、数据签名、数据脱敏。

（4）云原生计算环境安全

运行时安全：异常行为监控、入侵行为响应。

镜像安全：镜像扫描、镜像阻断、镜像访问控制、镜像安全通信。

编排及组件安全：基线扫描、漏洞扫描、敏感信息加密、访问控制、资源隔离与限制。

网络安全：入侵行为监控、访问控制、网络隔离。

（5）安全管理

身份管理、密钥管理、监控管理、安全审计、安全策略。

4.2.1.7.5 5G/6G 安全

(1) 5G 安全

(a)应用到的技术

终端和基站双向认证、切片隔离、用户数据和信令防护、用户标识保护、漫游安全、接口访问控制、软件数字签名、可信启动。

（b）防护方案

1)切片隔离方案

AMF 或 NRF 做访问频率监控并部署防火墙，防止恶意用户将公有 NF 的资源耗尽。

为终端接入不同切片通信配置不同的安全策略，为不同安全级别的切片设置不同的共用 NF。

切片内 NF 与外网设备之间部署虚拟防火墙或物理防火墙，保护切片内网与外网的安全。

通过网络划分、资源隔离、启用 SBA 访问控制来保证切片间 NF 的访问隔离。

通过 SBA 认证和 Oauth2.0 等授权机制，对不同切片的 NF 之间进行数据访问控制。

为用户提供切片隔离能力，包括不限于专用切片、部分逻辑共享切片、共享切片。对安全性要求高的切片，可以单独部署 vDC 和主机组进行物理隔离，对于安全和隔离要求一般的切片，可以划分单独 vDC，共用主机组进行逻辑隔离。

2) 增强身份鉴权方案

5G 网络提供主认证，支持 EPS-AKA’和 5G-AKA 认证机制对终端进行认证。

5G 网络支持二次认证，实现行业终端与外部 AAA 认证服务器的认证。

5G 网络提供 GBA 认证，智能终端或网关可以通过 GBA 与外部 AAA 认证。

支持定制 DNN 及切片，终端号码签约行业定制 DNN+切片。

实施基于位置的电子围栏终端安全接入，通过 AMF 进行小区 TA 和终端绑定，实现专网只允许合法授权终端接入。

部署零信任网关，进行终端接入的统一认证管理，避免非法终端接入。

3) 伪基站检测及防护方案

部署网管或信令监控系统，检测和定位伪基站：

a. 无线电检测：通过无线电设备检测来检测来自伪基站的无线电信号，参数包括：信号强度、周边基站、DBe 连续性、LAC/CELLID 连续性等。

b. 蜜罐技术：通过专用终端设备检测伪基站。

c. 客户投诉：根据突然的掉话以及信号不好，结合地理位置信息，定位伪基站的位置

配置网络流量监控系统，识别并标识网络中的一场流量波动，查看是否有不明基站迫使用户 UE 驻留。

使用终端设备向基站和网络发送测量报告，根据基站签名判断是否是伪基站。

4) 能力开放安全方案

根据 3GPP 定义的 CAPIF 框架，对 API 进行管理、发布和开放，应对 API 调用进行认证和授权。

边缘应用服务器调用运营商网络的能力开放功能，获取终端用户的敏感信息时，需要得到用户的授权同意。

部署防火墙、入侵检测等设备对关键 API 进行加固和安全防护。

5) 数据和信令保护方案

终端和 gNB/5GC 之间控制面进行加密。

终端支持机密和完整性保护算法，包括：NEA0，128-NEA1,128-NEA2 等。

终端内用户凭证的长期秘钥（K 值）使用防篡改组件进行存储，通过 HTTPS 加密传输。

终端与 5G 网络通信过程采用 SUCI 和 5G-GUTI，对 SUPI 进行加密保护。

归属网络公钥和 SUPI 保护方案应存储在终端 UICC 中，标识应存储在 UICC 中

gNB 与终端之间空口支持 AS 层 RRC 控制面信令和用户面完整性、机密性保护。

N2/N3 口部署 IPSEC。

6) 边缘平台安全防护方案

MEP 部署防 DDoS、链路加密、防重放等设备，MEP 和 APP 之间的数据传输应启

用机密性、完整性保护。MEC 应和 5G 核心网之间部署硬件防火墙，避免来自 5G 核心网的攻击。MEC 应和企业网络之间部署防火墙，防止来自企业网络的攻击。MEP 上部署的 APP 应使用 vFW 进行安全隔离，防止恶意 APP 攻击其他合法 APP。MEC 平台应部署虚拟化安全检测系统，防止来自虚拟机、容器的逃逸攻击。

(2) 6G 安全

6G 将通信的领域从物理世界进一步拓展到数字世界，通过在物理世界和数字世界中间提供即时、高效、智能的超链接来重塑世界。除了在 5G 网络要考虑的各方面安全措施外，6G 必须为未来量子计算、AI、海量连接以及各种远程车路协同、元宇宙等应用考虑安全防护。

（a）6G 安全架构

从架构上讲，6G 的安全进行的全新的设计和考量，包括内生安全、弹性安全、情景感知安全，多维数据安全和可评估安全等。内生安全包括安全的内化、研发过程的安全、安全的自适应、自生长、被攻击后的自愈合。弹性安全包括网络架构可编程级安全弹性部署，安全策略和可视化弹性业务发放等。情景感知安全包括智能化情景感知安全策略、情景切换情况下得自动安全策略转换以及安全策略可定制。多维数据安全包括时间维度的安全、空间维度的安全、传感维度安全以及立体隐私保护的安全。可评估安全包括网络整体架构安全可评估、网络协议安全可评估、业务场景安全解决方案可评估等。

(b) 6G 应用到的安全技术

除了 5G 网络的安全技术外，6G 要防范量子计算机的攻击，避免信息泄露、数据篡改，就要通过量子密钥、无线物理层密钥等增强的密码技术，为 6G 安全提供更强大的安全保证。6G 海量的终端接入，必须要采用轻量级接入认证、量子密钥、区块链等先进安全技术，实现移动终端、车机、物联网设备的安全接入与实时管控，为网络基础设施提供主动免疫能力。6G 更多的采用卫星通信，通信的密钥分发、传输链路的安全以及卫星、地面站的物理安全、防干扰，都是 6G 需要考虑的实际问题。

4.2.1.7.6 大数据安全

- 大数据采集安全

非法数据源识别、数据真实性分析、虚拟身份验证、数据分类分级、数据清洗、转换与加载。

- 大数据存储安全

大数据加密、磁盘存储安全、数据副本、数据归档、数据时效性。

- 大数据传输安全

数据属性加密、可搜索加密技术、全同态加密、隐私保护公开验证、通道安全、接口安全、审核与监控。

- 大数据使用和开放安全

大数据安全访问控制、信息流安全控制、数字水印技术、大数据隐私保护模型、数据匿名化技术、导入导出安全、数据交换监控

- 大数据安全销毁与删除

介质管理、介质销毁、数据销毁技术

- 大数据安全处理

分布式处理安全、数据分析安全、数据正当使用、密文数据处理、数据脱敏处理、数据溯源

4.2.1.7.7 工控安全

工控安全解决方案涉及以下应用技术：工业网络安全风险评估平台、工业安全扫描平台/工控安全检测、工业防火墙、工业主机安全、工业资产测绘平台、工业等保工具箱、工控安全审计、工控靶场、工控安全管理平台、工控安全培训、工控靶场、工控网闸。

4.2.1.7.8 视频安全

视频安全解决方案涉及以下应用技术：视频防火墙、视频设备安全准入、视频防泄漏平台、视频转码接入网关、视频综合安全网关、视频加密网关

4.2.1.7.9 云安全

云安全解决方案涉及以下应用技术：多云管理平台、多云安全中心、云基础构架安全、云原生安全、云应用安全、云平台安全运营。

4.2.2 数字安全产品

4.2.2.1 端点安全

端点安全包括“恶意软件防护”、“终端安全管理”和“其他”三个二级分类，每个二级分类下有几个三级分类从属于二级分类。三级分类的这一部分需要解释终端检测和响应，这是国外市场的热点，有很大的趋势取代反病毒产品。

4.2.2.2 网络安全

网络安全包括“安全网关”、“入侵检测与防御”、“网络监控与审计”和“其他”四个二级分类，这是市场份额最大的一大类。

这部分的三级分类需要说明的是：

- 虚拟专用网暂时被列为关中安全网，因为几乎所有的防火墙产品都有虚拟专用网功能，虽然独立的 VPN 产品已经开发了一些专有的功能，比如认证和权限管理、应用虚拟化等等；
- 高级威胁检测（APT）产品虽然结合了行为分析、威胁情报和沙盒的特点，主要针对“0 day”利用问题，但本质上是检测入侵行为被归为入侵检测和防御范畴；
- 在国内，在线行为管理也是一大类，因为销售许可证的申请一般是按照网络传播的审核标准进行审核，所以分为行为管理和审核。

4.2.2.3 应用安全

应用安全包括“WEB 安全”、“数据库安全”和“邮件安全”三个二级分类。

4.2.2.4 数据安全

数据安全包括“数据治理”、“文件管理与加密”和“数据备份与恢复”三个二级分类，数据是国家、企业和个人的核心资产，在大数据时代的数据安全尤为重要，数据治理主要可以用 DLP 产品解决数据控制的问题。

4.2.2.5 身份和访问管理安全

身份和访问管理安全包括两个二级分类，即“身份验证和权限管理”和“高级身份验证”，基本围绕三个问题：“你是谁？”是认证问题；“你能怎么办？”这是权威问题；“你做了什么？”这是审计问题。

4.2.2.6 安全管理

安全管理包括“安全运行和事件响应”、“脆弱性评估和管理”以及“治理、风险和合规”三个二级类别。日志审计 LA、安全信息和安全运营中心的 SOC 和事件管理的 SIEM 的区别在于 LA 的数据源是日志，主要流程是采集处理、分析呈现。除了日志，SIEM 的数据源还应该有流、dpi 和完整包、注册表、进程等对采集、处理和分析能力的要求更强，显示内容比 LA 更完整、更丰富。SOC 是在 SIEM 的基础上增加工作流，最新的特

点是安全自动化和协作。国内此类产品的数据采集维度相对单一(主要是日志)，在数据处理分析能力、安全自动化、协作等方面还有进一步提升的空间。再说漏洞扫描和补丁管理，不久前，Wannacry 还是个 N day 漏洞，只要及时打补丁，什么都不会发生。对于一般用户来说，及时的安全更新将大大降低安全风险。如果值得使用 0 day 易受攻击，你必须考虑更高级别的安全措施。

表 4-1 ：常见网络安全产品分类

安全大类	产品品类
端点安全	● 防病毒软件 ● 主机检测与审计 ● 安全操作系统 ● 主机/服务器加固
网络安全	● 防火墙 ● 入侵检测与防御 ● 网闸 ● 防病毒网关 ● 上网行为管理 ● 网络安全审计 ● VPN ● 网络准入
应用安全	● Web 应用防火墙 ● Web 应用安全扫描 ● 网页防篡改 ● 邮件安全
数据安全	● 数据库审计与防护 ● 安全数据库 ● 数据泄露防护 ● 文件管理与加密 ● 数据备份与恢复
身份访问管理	● 运维审计堡垒机 ● 数字证书 ● 身份认证与权限管理 ● 硬件认证
安全管理	● 安全管理平台 ● 日志分析与审计 ● 脆弱性评估与管理 ● 安全基线与配置管理 ● 威胁分析与管理 ● 终端安全管理

4.3 数字安全服务

4.3.1 安全服务供应概述

根据数字安全框架，数字安全概念包括了网络安全、信息安全、数据安全、隐私保护、元宇宙、数字身份、原生安全等领域。其中，对于元宇宙等新兴概念，业界尚在研究探索阶段，尚未发展出成熟的安全服务（尽管对新概念的研究本身就可作为一项服务交付，但研究的主题是高度定制化的）。其余数个领域的理论、实践与技术均已经过多年的发展，已具备较成熟的服务和产品供给。

根据 IDC 对安全服务的定义，安全服务关注的重点是 IT 系统的实施、管理、运营和审计，以确保物理和数字资产和/或敏感信息的安全。安全服务涉及跨企业信息技术基础设施规划、设计、构建和管理信息安全所需的所有活动的整体视图。

根据 IDC 的安全服务分类方法，数字安全服务可划分为三大类：

- 专业安全服务（Professional Security Services）
- 部署与培训（Deployment and Training）
- 托管安全服务（Managed Security Services）

在这三大类别下，可以依次再分解二级和三级类别。例如专业安全服务下可再分为顾问服务（Consulting）和实施与集成服务（Implementation and Integration），安全管理服务下可再分为客户场所设备（MSS-CPE, customer premise equipment）、传统托管（MSS-Traditional Hosted）、云托管（MSS-Cloud Hosted）。

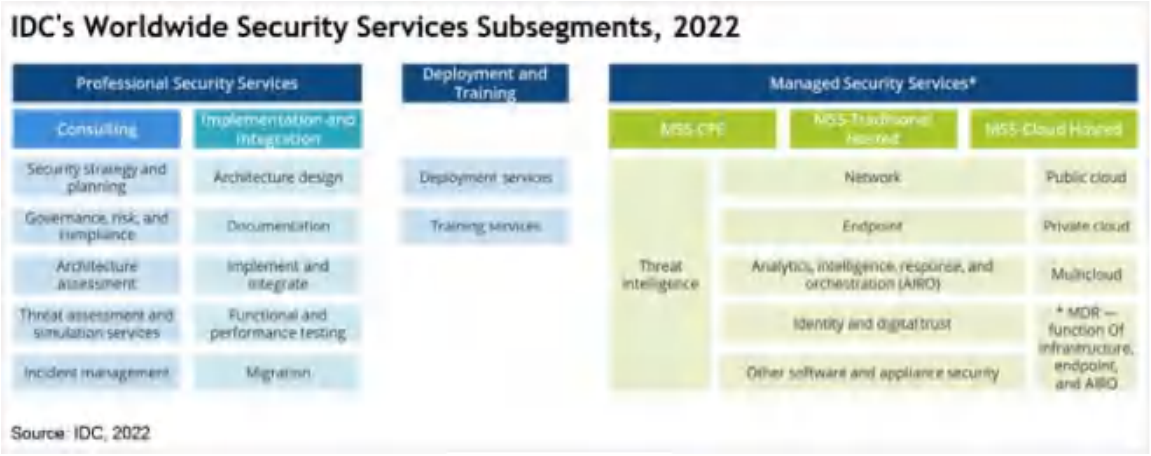


图 4-13 IDC 世界范围安全服务 2022[15]

[15] IDC's Worldwide Security Services Taxonomy, 2022

Gartner[16]也曾定义过安全服务的几个分类，包括：

- 硬件支持（Hardware Support）
- 咨询（Consulting）
- 实施（Implementation）
- IT 外包（安全外包和托管安全服务）（IT Outsourcing (Security Outsourcing and Managed Security Services)）

(参考来源：Gartner: https://www.gartner.com/en/documents/3885567)

对比 Gartner 和 IDC 的分类方法，两者在大类划分上基本保持一致。

鉴于硬件支持、部署、实施等服务是软/硬件供应商、集成服务商以及它们的分包商提供的通用服务，本质上是为了支撑安全产品和技术的安装、配置，以及跨系统间的集成，其本质和其他 IT 产品和技术的部署、实施与维护服务没有差别，组织可以很便利地从设备厂商或集成服务商处获得这些专业服务。因此，本报告并不会在部署、实施和软硬件支持的角度下对安全服务展开叙述。

从广义来看，针对安全的培训和认证服务毫无疑问也是一种安全服务，为保持本报告内容结构的连贯性，培训和认证的相关服务内容将在后续章节单独叙述。

另外，有部分服务商把一些传统上需要现场交付的安全服务进行了云服务化，通过精心设置的门户网站，让客户实现在线自助服务。客户使用服务商提供的 SaaS 产品完成诸如漏洞扫描、威胁情报、日志分析等工作，并根据服务的内容和工作量支付费用。这种创新的交付方式模糊了传统意义上的产品和服务边界，大大丰富了安全服务的场景。

4.3.2 主流的数字安全服务

数字安全服务类型和交付方式灵活多变，不同服务商的服务目录可能存在很大差异，并且可以针对不同的客户高度定制化，本报告尽可能地依据大众认可的分类框架，来对数字安全服务及市场上的主要供应商进行介绍。

4.3.2.1 安全咨询服务 Security Consulting Services

安全咨询是与信息和 IT 安全设计、评估和建议相关的咨询服务，目的是使特定客户组织得到可接受的安全风险水平。安全咨询服务是一系列专业服务活动的组合，典型的服务内容包括安全策略和规划、治理风险和法规遵循(GRC)、系统架构评估、威胁评估

[16] Gartner: https://www.gartner.com/en/documents/3885567

和事件模拟、安全事件管理等。

安全咨询服务商往往具备多种服务能力，因为寻求咨询服务的客户需求是高度差异化的，咨询服务商必须具备非常广阔的安全管理和安全技术知识，才能提供让不同需求的客户满意的解决方案或专业意见。这种广阔的安全知识和丰富的行业经验也让安全咨询服务商发展出多样化的服务组合。

安全战略及规划	帮助客户建立战略路线图，以改善组织的整体安全态势。
治理、风险与合规	专注于组织在**网络安全、隐私、网络风险和网络审计**方面解决本地或国际合规框架的复杂需求。
架构评估	架构评估侧重于对组织的整体架构进行深入评估，并确定技术和流程的路线图，以改进安全态势。
威胁评估与模拟	旨在通过模拟恶意黑客的攻击来评估企业资源的安全性，以识别和评估更有可能发生攻击的脆弱区域。
事件管理	服务包括制定事件响应计划，通过红/蓝/紫队对计划进行评估并加以改进，通过取证服务来确认网络攻击的原因与性质，并从数字媒介中获取与安全事件相关的信息和证据。

表 4 –2 典型的安全咨询服务类型[17]

国际上提供综合安全咨询服务的主要供应商包括（按首字母排列）：

- **Accenture Cybersecurity Consulting Services**

埃森哲致力于提高客户对网络威胁的抵御能力，以匹配客户业务生态系统和价值链的扩大，为客户的特定业务需求量身打造网络安全。广泛的网络安全知识和深厚的行业专业知识使埃森哲能够开发下一代网络安全服务，从端到端保护客户的业务。

- **Deloitte Security Consulting Services**

德勤帮助企业防范网络攻击，保护宝贵资产。德勤相信要做到安全、警惕和灵活，不仅要着眼于如何预防和应对攻击，还要着眼于如何管理网络风险，使客户能够释放出新的机会。

- **EY Security Consulting Services**

安永网络安全、战略、风险、合规和弹性团队帮助组织在推动业务增长和运营战略

[17] IDC's Worldwide Security Services Taxonomy, 2022

的背景下评估其网络安全和弹性项目的有效性和效率。这些服务可适用于各种应用场景（信息技术、物联网、运营技术、云等），为组织提供了明确的风险度量和风险捕获，并展示了未来将如何管理网络风险。

- **IBM Security Consulting Services**

提供全球安全咨询专业知识，全面的能力和可靠的方法，以保护客户的业务，帮助首席安全官、公司高管和董事会成员将安全融入业务战略、流程和系统。

- **KPMG Cyber Security Services**

毕马威的成员公司拥有从董事会到数据中心的全方位专业知识。除了评估客户的网络安全并将其与业务优先事项相结合外，还帮助客户制定先进的解决方案，实施这些解决方案，监控持续的风险，并帮助客户有效应对网络事件。

- **Kroll Security Consulting Services**

Kroll 的整体安全咨询服务包括当前和新出现的威胁评估、政策审查和发展以及总体规划，可以通过包括威胁评估、策略审阅和开发，以及总体规划在内的服务，帮助客户构建一个强大的安全环境。

- **Protiviti Security Consulting Services**

Protiviti 的网络安全咨询服务具有战略和战术两个层面的功能，将深厚的技术能力与高层沟通和管理相结合。Protiviti 的主题专家通过实施网络安全计划、网络安全标准、执行渗透测试、或处理数据泄露事件等活动，帮助客户了解他们的网络风险和解决他们的需求。

- **PwC Security Consulting Services**

普华永道帮助客户推动可持续增长，保护价值，并通过建立信任和增强对中断、变化和网络威胁的抵御能力来应对不确定性。

4.3.2.2 托管安全服务 Managed Security Services

托管安全服务商(MSSP)提供安全设备和系统的外包监控和管理。常用服务包括防火墙管理、入侵检测、虚拟专用网、漏洞扫描和防病毒服务。MSSPs 使用高可用性安全操作中心(从他们自己的设施或从其他数据中心供应商)提供 24/7 服务，旨在减少企业需要雇用、培训和保留的操作安全人员数量，以保持可接受的安全态势。托管安全服务涵盖了所有安全运营服务的变体，并且在服务场所上有多种不同选择（例如在客户自有场所、在第三方场所、在云端等）。

尽管对于托管安全服务可以按不同的维度划分为多重子类，但这种分类更多是从工作团队分工和交付方式的角度来考虑。从客户的角度，往往只关注服务交付的最终结果，要求服务商的具备全面的综合服务交付能力。服务商则根据客户的要求提供各种灵活定制化的服务组合，这些服务组合的内容与客户的安全运营职责划分密切相关。因此，并无必要对托管安全服务进行细分的叙述，而可将其作为一个整体服务进行考虑。

国际市场上提供托管安全服务的主要服务商包括（按首字母排列）：

- **Accenture Managed Security Services**

通过创新性的技术、as-a-Service 能力和网络安全服务组合，帮助客户快速扩展安全与合规运营。

- **BT Managed Security Services**

BT 拥有大量的托管安全服务组合，包括网络安全解决方案、威胁检测和响应解决方案、云安全解决方案、端点安全、安全咨询服务等。

- **IBM Managed Security Services**

可以通过定制服务增强客户的安全计划，包括威胁、云、基础设施、数据、身份和响应管理。IBM MSS 专家可以帮助长期优化、微调和提高安全程序效率，帮助客户解决从最简单到最复杂的安全需求，全天候监视和管理安全事件。

- **NTT Security Managed Security Services**

通过高级威胁情报和高级分析来保护和优化客户组织。组织可利用 NTT 托管安全服务将数据转化为知识，并获得组织的整个安全图景的可见性，而不是孤立的事件。

- **Secureworks Managed Security Services**

为客户不断扩大的网络提供全天候监控和管理的安全服务。客户可以通过 Taegis 安全分析和运营平台获得全面的托管解决方案，提供跨端点、网络和云环境的高级威胁搜索、检测和快速响应。

- **Trustwave Managed Security Services**

Trustwave 托管安全服务可以帮助客户扩展其团队的能力，强化环境，并随着时间的推移变得更有弹性。在精英团队提供的全球威胁情报的支持下，全面而灵活的托管安全服务帮助客户抵御高级威胁，减少其攻击面，识别新的风险，响应事件并从中恢复。

- **Verizon Managed Security Services**

Verizon 为客户不同位置的各种安全设备提供监视和管理。客户的设备通过连接套

件连接到安全管理中心的本地事件采集器。这种与供应商无关的服务允许客户选择世界级的产品，帮助保护技术投资，并避免供应商锁定。

- **Wipro Managed Security Services**

Wipro 的托管安全服务包括先进的网络防御中心、网络安全平台以及托管安全基础设施和运营，在不影响业务性能的情况下提供持续的、实时的保护。

4.3.2.3 云安全服务 Cloud Security Services

当云计算成为了数字化时代的基础设施基石，云安全就成为了安全服务发展的焦点之一。云安全服务以云计算的方式提供，不仅仅可以保障云上资产的安全性，还可以发挥云服务的特点，通过网络和 API 将安全保护功能覆盖到组织的本地资产，实现安全即服务(Security as a Service)。在前述的安全产品、方案和服务中，有许多是可以通过云服务的形式提供给客户，并往往支持多种部署模式。

几大主要云服务商均提供了大量的云安全服务，使客户在构建云基础设施时，能以便利的方式获取到最适配其云架构的安全解决方案，最大限度地增强云基础设施、数据和应用程序的安全性。

国际上几大云服务商提供的安全服务能力有（按首字母排列）：

- **Alibaba Cloud**

阿里云对客户的业务进行安全评估，分析业务需求，并与客户紧密合作，定制无缝适合业务的安全规则。阿里云原生安全服务是基于自适应安全架构开发的，这些服务支持对客户数据进行持续的安全监控和分析。阿里云管理基础设施，并为其服务提供安全保障。此外，阿里云还制定了服务交付流程，确保阿里云提供的所有服务都是安全可靠的。

- **AWS**

AWS 客户受益于 AWS 的数据中心和用于保护信息、身份、应用程序和设备的网络架构。通过 AWS 的全面服务和特性，组织可以提高他们满足核心安全性和遵从性需求的能力，例如数据局部性、保护和机密性。

- **Microsoft Azure**

根据云服务模型的不同，谁负责管理应用程序或服务的安全性有不同的职责。Azure 平台中有一些可用的功能，通过内置的特性以及可以部署到 Azure 订阅中的合作伙伴解决方案，来帮助企业履行这些职责。内置功能按六个功能区域组织:操作、应用程序、

存储、网络、计算和身份。.

- **Google Cloud**

Google Cloud 的安全解决方案可以应用于云、本地部署或混合部署。在攻击造成损害或损失之前，检测、调查并帮助阻止针对业务和用户的网络威胁。

Google Cloud 提供的服务可以帮助客户保护他们的应用程序免受欺诈，帮助检测和调查威胁；并使用谷歌依赖的相同的按设计安全的基础设施来保护用户、数据和应用程序；Google Cloud 的私有软件定义网络为世界各地的用户提供快速可靠的连接。.

- **IBM**

IBM 认为，企业在迁移到云时将面临新的网络安全挑战，在迁移到混合云环境时，企业需要保持可见性、控制和安全性。在云转型之旅的每个关键阶段，组织都需要安全管理来领先于高级威胁。IBM 提供综合性的云安全服务，包括安全策略、云本机安全、容器安全解决方案等。

- **Oracle**

Oracle 云基础设施(OCI)安全帮助组织降低云工作负载的安全威胁风险。通过将简单、规范和集成的安全能力内置到 OCI 平台中，Oracle 帮助客户轻松采用和保护他们的云基础设施、数据和应用程序。

4.3.3 数字安全服务的发展机会与趋势展望

在当今数字经济的浪潮下，全球企业依托不断涌现的数字化技术实现商业运营模式的颠覆性变革，以期在激烈的市场竞争中获得优势，使企业有机会以超越历史的速度和规模实现收益。在数字化商业模式下，各种计算资源和设备通过高速网络进行连接，企业在享受数字经济收益的同时，也使其关键数字资产暴露在网络攻击的严峻威胁之下。

根据安永 2020-2021 全球信息安全调查报告，全球受访的 CIO/CSO 们认为，降低持续涌现的安全威胁所带来的风险是企业增加信息安全投入的最重要驱动因素，而合规和监管要求带来的挑战则排在第二位。但是，这两项驱动因素的重要比例均呈现下降趋势，特别是监管合规方面，CSO 们感到越来越难通过合规项目获得公司的资金投入。尽管高达 49%的受访者称，确保合规可能是工作中压力最大的一部分，但认为能够以监管合规理由向董事会成功申请到额外预算的受访者只有 18%，而 2020 年这一比例为 29%。

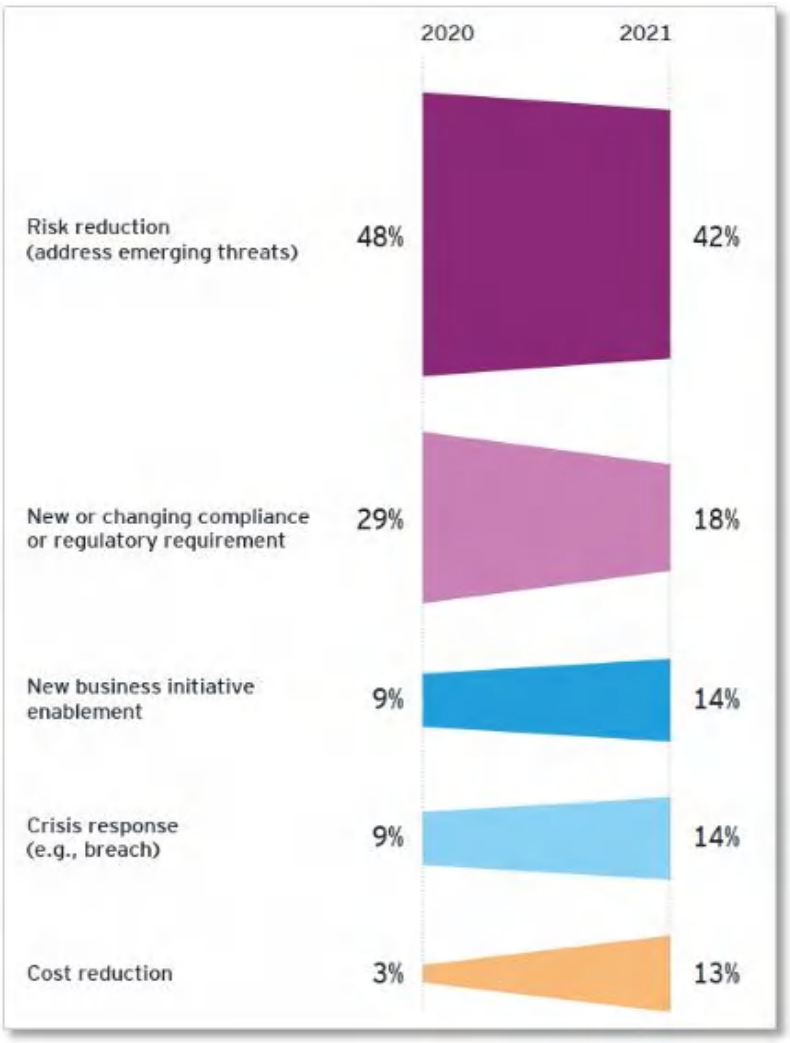


图 4-14 企业新增网络安全开销的主要驱动因素[18]

来自客户企业的意见对安全服务市场的发展可起到一定的预示作用。自 2018 年 GDPR 生效后，全球多个主要国家掀起个人信息保护立法的潮流。企业为了满足在各国的隐私合规要求，投入了大量资源和精力用于业务流程和信息系统改造，这曾在安全服务市场上带来一波相当规模的需求。在未来数年，这股需求热度可能将随着监管要求的逐渐清晰，以及企业业务流程和系统的合规化改造愈加成熟而逐渐降温，变为企业的日常运营工作。而 COVID-19、供应链危机、全球网络攻击等一系列事件给企业带来的生存压力却是残酷而真实。沉重的企业压力无疑将传递到安全管理部门，影响着企业对未来数字安全服务的需求。

为了能有效保护关键数字资产的安全能力，企业需要投入大量的资源、精力和时间来进行能力建设和持续运营，这未必能够快速见效，并且会影响到企业在其他经营管理

[18] EY: Global Information Security Survey (GISS) 2020-2021

领域的投入。因此，通过采购安全专业服务，以灵活的方式实现安全能力的快速构建，成为了众多企业的明智选择。

根据多家市场调研机构的数据显示，全球的安全服务市场呈现不断增长的趋势。

根据 Statista 对 2011-2020 全球安全服务市场的统计，在全球范围内的安全服务市场份额从 2011 年的 780 亿美元上升至 2020 年的 1320 亿美元。其中北美与亚太区市场实现了较大程度的增长。

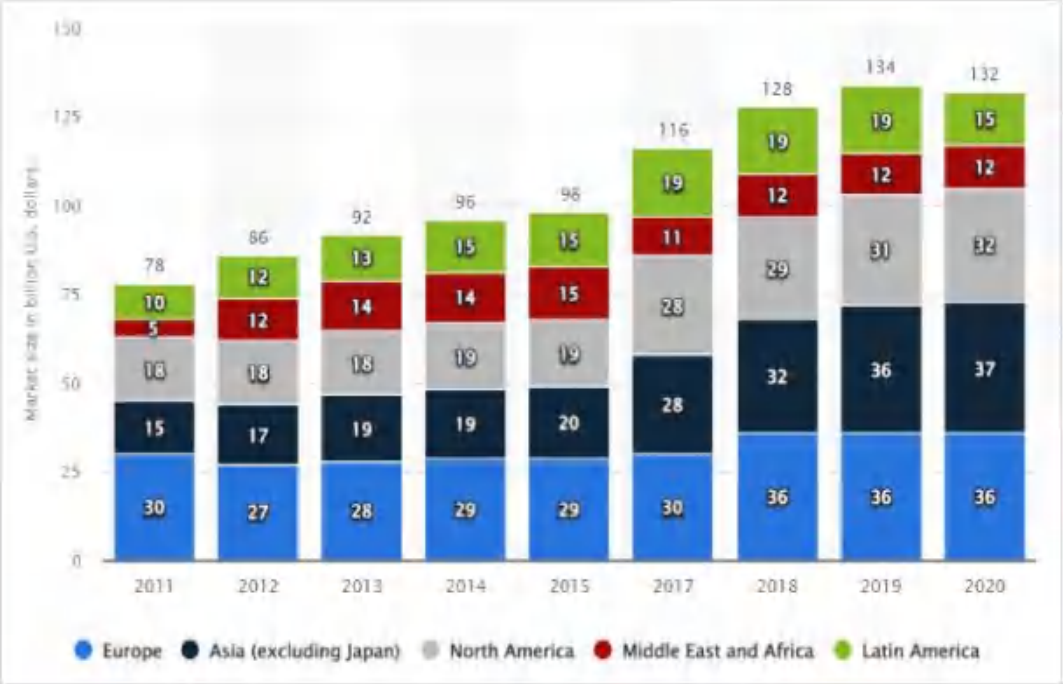


图 4-15 世界范围内安全服务市场规模统计， 2011 - 2020 年[19]

根据 IDC 的一项研究，全球安全服务市场在 2021-2025 年区间将获得 10.7%的平均增长率，其中增幅最大的是托管安全服务市场，增幅达 13.3%，其次是咨询服务，增幅达 10.7%。

[19] Security services: global market size 2020 | Statista

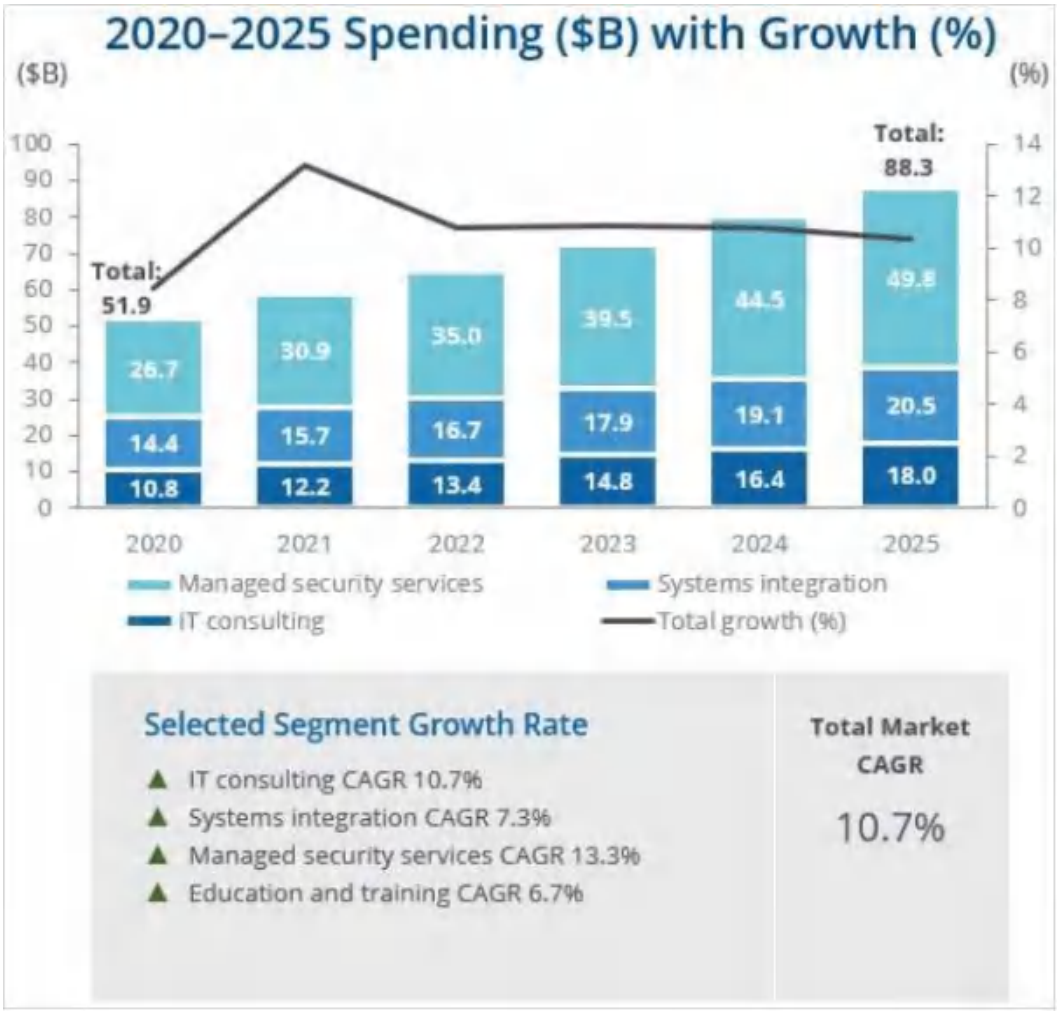


图 4-16 世界安全服务市场预测，2021 - 2025 年[20]

根据 Mordor Intelligence 的预测，未来数年间，亚太区的安全市场份额将保持高速增长，北美和欧洲将得到中等程度的增长。

[20] Worldwide and U.S. Comprehensive Security Services Forecast, 2021–2025: Growth Continues During and Beyond COVID-19 (idc.com)

图 4-17 世界不同地区的安全服务市场增长预测， 2021 - 2026 年[21]

根据 Gartner 一份对未来安全服务发展趋势的研究报告[22]，未来几年，安全服务的格局将发生重大变化，安全技术供应商和服务供应商的产品领导者必须调整服务交付策略，因为买家寻求将内部业务成果的运营交付转移到服务供应商。Gartner 的研究员预测，

- 到 2025 年，超过 25%的技术供应商将提供供应商交付的服务包，高于 2021 年的 10%。
- 到 2026 年，超过 50%的服务供应商将重新调整业务组合，以提供基于用例的结果（use-case-based outcomes）。
- 到 2028 年，80%的安全服务外包将流向提供基于用例结果的供应商，而 2021 年这一比例不到 5%。

新兴数字技术仍在不断涌现和发展，创造性的数字经济概念仍在不断孵化。毫无疑问，数字安全服务的类型和交付方式也将不断演变，其市场规模必将伴随数字经济的发展而不断壮大。对于安全服务供应商而言，这当然是一个巨大的市场机会。对于企业而言，采购安全服务可以作为本身安全能力的快速补充和有效增强，使企业在不断应用新兴数字技术来重铸商业模式和流程的过程中，仍动态保持对各种新型安全风险的有效管

[21] Management Consulting Services Market Share, Trends | 2022 - 27 | Industry Growth (mordorintelligence.com)

[22] Gartner ID G00752203 - Emerging Trends: Future of Security Services - By Shawn Eftink, John Collins - 24 Nov 2021

理，为企业在数字经济浪潮中保驾护航。

4.4 数字安全教育

4.4.1 数字安全教育定义

数字安全是一个集合术语，描述用于保护在线身份、数据和其他资产的资源。这些工具包括网络服务、防病毒软件、智能手机 SIM 卡、生物识别和安全个人设备。

在计算机网络时代，维护适当安全性所需的具体过程存在显著差异。只要一不小心，一个拇指大的 U 盘就可能会泄露数百万条记录。通过一根网线就可以把敏感材料分享给数千万用户。

虽然这些场景可能看起来不祥甚至可怕，但它们只是故事的一部分——事实上，只是一小部分；在未经培训的用户手中，同样的技术可能会引起如此多的关注，但如果使用得当，这些技术实际上可以比以往任何时候都更安全地保护信息。因此，数字安全教育在数字安全方面起到了至关重要的作用。

4.4.2 数字安全教育的现状

目前数字安全教育基本通过国际和国内两个信息安全专业认证体系开展。

4.4.2.1 国际信息安全认证体系

（1）CSA 云安全联盟

国际云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于 2009 年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字技术与安全产业产业发展。国际云安全联盟大中华区（CSA GCR）作为 CSA 全球四大区之一，2016 年在香港独立注册，于 2021 年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际 NGO，旨在立足中国，连接全球，推动大中华区网络安全技术标准与产业的发展及国际合作。

CSA 聚焦在云安全领域的基础标准研究和产业最佳实践，其发布的《云计算关键领域安全指南》是云安全领域奠基性的研究成果，得到全球普遍认可，《云控制矩阵（CCM）》被世界各国认为全球通用的黄金标准。

CCSK（云计算安全知识认证）

CSA 于 2010 年推出 CCSK，被誉为“云计算认证之母”，是云安全从业人员必备证书之一。成千上万的 IT 和安全专业人员通过 CCSK 认证，提升云安全专业技能，助力职业生涯发展。

CCSK 的培训内容从云计算的架构框架开始，涵盖了数据安全、治理与企业风险、可交互性与可移植性等 14 个领域，详细讲解了真实云计算环境中的安全问题及其解决方案。

目前全国已有大约 2000 多人获得 CCSK 证书。

取得 CCSK 认证意味着应试者成功通过了考试并充分理解了 CSA 指南及 ENISA 白皮书中所有核心概念，能够正确采取合理手段保证云计算环境的安全问题。

CZTP（零信任认证专家）

零信任认证专家是零信任领域首个面向从业人员的安全认证，涵盖最新的国际零信任架构技术与实践知识，旨在为网络信息安全从业人员在数字化时代下提供零信任全面的安全知识，培养零信任安全思维，传播与践行零信任理念，为企业守护核心数字资产。

CDSP （数据安全认证专家）

CDSP 针对云数据安全、ICT 数据安全和新兴热点业务的数据安全（如 AI / IoT）展开阐述，并结合各类新兴技术的不同场景，给出数据安全架构、安全设计、隐私保护的一般原则和业界最佳实践，旨在确保信息安全、数据安全、云计算、隐私保护的从业人员对数据安全威胁和数据安全框架和最佳实践有系统性地认知并掌握基本技能，并具备安全设计、审计、评估和保护数据与隐私所需的关键知识、技能和能力，可以将相关知识和技能落实到日常工作中，帮助企业满足相关法律法规和监管要求。

CBP（区块链专业人员认证）

CBP 由云安全联盟推出，涵盖最新的区块链原理与实践知识。作为 CSA 区块链首个个人安全认证，旨在为 IT 从业人员在数字化时代下提供全面的区块链原理及安全思维，理解和掌握区块链、密码技术、共识机制、激励机制、智能合约、P2P 网络等的基本原理和实践应用，培养其应用区块链原理，准确分析各行业中存在的去中心化信任、公开透明、不可篡改、不可伪造以及跟踪溯源等安全问题，设计和使用区块链技术解决各行业应用问题。

CDPO （认证数据保护官）

CDPO 聚焦数据法律法规剖析、隐私保护合规体系建设以及梳理并理解数据治理和信息安全的基本概念，打造综合性的专注中国特色的个人信息保护实操培训课程体系。CDPO 旨在促进数字化领域从业人员对中国法律、法规的理解及隐私保护意识，主动跟踪合规要求变化，梳理内部的合规差距，真正能设计和落实具体的合规管理和技术措施进而规避合规风险，充分应用到工作中。

CCPTP （认证云渗透测试专家）

CCPTP 旨在提供针对云计算渗透测试所需的专业实操技能，弥补云渗透测试认知的差距和技能人才培养的空白，提升专业人员能力及提供认证证书，为云计算产业发展提供渗透人才队伍保障。认证课程包含了云渗透测试知识体系、测试流程、实践技术、法律法规、渗透测试人员道德规范、渗透测试方法论 以及实操技术等内容。

ACSE （高级云安全专家）

ACSE 旨在培养数字化时代云原生环境及 DevSecOps 环境的安全专家，解决如何做好新一代云原生安全及 DevSecOps 安全的问题。通过课程学习掌握最新的云原生的安全防护管理体系与专家级的评估方法、业内先进的 DevSecOps 安全的实现模型与技术，以及云运维与事件响应与云安全合规与审计的最新方法。ACSE 是集云安全、云原生、与相关新兴技术安全于一体的高级云安全专家认证

（2）ISACA

ISACA®(国际信息系统审计协会)是全球公认的 IT 治理、网络安全、审计与鉴证、风险控制、数据隐私保护以及标准合规的领导组织，会员遍布逾 180 多个国家，总数超过 150,000 人。ISACA 提供的主要认证有：

CISA （国际信息系统审计师）

CISA（Certified Information Systems Auditor，中文为国际信息系统审计师）认证是由信息系统审计与控制协会 ISACA（Information Systems Audit and Control Association）发起的，是信息系统审计、控制与安全等专业领域中取得成绩的象征。CISA 认证适用于企业信息系统管理人员、IT 管理人员、IT 审计人员、或信息化咨询顾问、信息安全厂商或服务提供商、和其他对信息系统审计感兴趣的人员。

CISM （国际注册信息安全经理）

ISACA 创立的注册信息安全经理认证(CISM)，聚焦在信息安全战略、评估系统和政策，自 2002 年推出后，受到了全球资深信息安全经理们的推崇，迄今已有超过 28,000 人获得了这一证书。CISM 注重管理层面，是全球公认的对开发、建立和管理企业信息安全系统的个人能力的认可。CISM 证书的维持率超过 95%。

注册信息安全经理(CISM)针对信息安全风险在业务应用的管理和相关问题的解决，CISM 为信息安全经理和信息安全管理职责的专业人员量身定制，提升企业总体的信息系统安全管理水平，向高级管理层确保：拥有 CISM 专业资格认证的人员具有知识和能力提供有效的信息安全管理和咨询，以业务为导向，在应用于业务的管理、设计和技术安全问题时，强调信息风险管理概念。CISM 不适用于信息系统审计人员，但对具有信息系统管理经验和责任的信息系统审计师同样有益。

CGEIT（国际注册企业 IT 治理证书）

ISACA 的 CGEIT 国际注册企业 IT 治理证书自 2007 年推出以来，全球已有 8,000 多名

专业人士通过了该 认证，展现了他们在实现与企业战略目标相一致的包括 IT 在内的全面治理中所具备的知识、能力和经验。在数字化转型中，随着新技术的出现和应用，董事会和高管不得不制定和实施有效的治理和业务连续性计划。CGEIT 持证人员可以完美介入，确保采用恰当的系统和流程，可以灵活调整和继续运营，降低干扰。作为第一个也是唯一一个面向 IT 治理专业人士的认证，CGEIT 可以让持证人员掌握评估组织需求和风险偏好的全面知识，获取高层管理人员支持，以及将 IT 部门转变成为价值中心的能力。

CRISC（国际注册风险和信息系统控制）

随着全球安全漏洞的急剧增加，对了解 IT 风险及其与组织关系的专业人员的需求越来越大。ISACA 的风险和信息系统控制认证(CRISC)帮助专业人士发展相关技能，满足这一需求。CRISC 向 IT 专业人士提供专业知识，使他们能够识别、评估和管理 IT 风险，同时计划和实施控制措施和框架。它还可以帮助个人建立一种通用的语言，在 IT 部门内部和整个组织内就安全和系统控制进行沟通。 该认证针对 IT 以及商务人士，包括风险与合规人士、业务分析师、项目经理，以及所有通过开发、实施和维护信息系统控制从而发现和管理风险的专业人士。

CDPSE（国际注册数据隐私专家认证）

ISACA 的 CDPSE 国际注册数据隐私安全专家证书自 2020 年推出以来，全球有超过 20,000 名专业人士获 得了认证，证明了他们跨部门合作的经验和能力，以及对合规要求的理解和实施恰当隐私控制 的能力。CDPSE 认证帮助企业中的技术、安全、法律及合规人员更好地掌握数据隐私保护所涉及的相关管理和技术能力，助力企业更好落地隐私

保护管理措施和技术方案，从而构建并提升更全面的数据隐私保护体系以应对不断变化的外部监管环境。持有 CDPSE 证书可以证明您建立和实施全面的隐私解决方案的经验和能力，弥合了隐私合规性的技术和法律方面之间的鸿沟。CDPSE 适合在 IT、运营、信息安全、系统和应用开发、企业架构和项目管理等部门工作负责落实一线防御的专业人员，负责评估和确保法务和合规的专业人员，负责隐私保护政策和流程的开发、实施和运维的专业人员，与信息技术和数据治理流程打交道的人员，负责评估隐私保护实践以及合规，与审计和风险管理流程打交道的专业人员。

（3）(ISC) ²

(ISC)²®(国际信息系统安全认证联盟) 成立于 1989 年，是全球最大的网络、信息、软件与基础设施安全认证会员制非营利组织，是为信息安全专业人士职业生涯提供教育及认证服务的全球领导者。(ISC)²(总部位于美国，区域办公室设在伦敦、香港及北京（授权中国代理办事处）。(ISC)² 以其一流的信息安全人才教育与培养计划，以及“金牌标准”安全认证而享誉全球。(ISC) ²提供如下认证：

CISSP（注册信息系统安全认证专家）

CISSP 即注册信息系统安全认证专家是目前世界上最权威、最全面的国际化信息系统安全方面的认证，由国际信息系统安全认证协会(ISC)²组织和管理，(ISC)²在全世界各地举办考试，符合考试资格的人员在通过考试后被授予 CISSP 认证证书。

CISSP 可以证明证书持有者具备了符合国际标准要求的信息安全知识水平和经验能力，提升其专业可信度，并为企业和组织提供寻找专业人员的凭证依据，目前已经得到了全世界广泛的认可。越来越多的公司要求自己和合作伙伴的员工拥有 CISSP，该资质持有者目前供不应求。目前全国已有大约 3000 多人获得 CISSP 证书。

取得 CISSP 认证，表明持有者拥有完善的信息安全知识体系和丰富的行业经验，以

卓越的能力服务于各大 IT 相关企业及电信、金融、大型制造业、服务业等行业，CISSP 的工作能力值得信赖。

(ISC)² CCSP® (Certified Cloud Security Professional，注册云安全专家）认证旨在满足云计算市场对合格安全人才的关键需求，并反映最新、最全面的云安全最佳实践。获得全球认可的 CCSP 云安全认证是建立您的职业生涯和更好地保护云中关键资产的有效途径。

CCSP 表明持证者拥有先进的技术技能和知识，能够使用(ISC)²的网络安全专家制定的最佳实践、政策和程序设计、管理和保护云中的数据、应用程序和基础设施。

(ISC)²® 注册软件生命周期安全师（Certified Secure Software Lifecycle Professional）(CSSLP®) 是信息安全行业唯一一个针对保障整个软件开发生命周期安全性的国际认证。

此资格认证制定了从概念到规划、运行、维护直至废弃处理在内的软件开发各阶段保证安全性的行业标准和最佳实践。安全性的核心理念包含机密性、完整性、实用性、验证、授权与审计，在软件开发生命周期中缺一不可。若不严守以上原理，信息将受到严重威胁。实践证明，在软件生命周期初期就考虑安全性并在各阶段保持安全性的方式，比当今常用的先发布后打补丁的方式，不但能节省 30-100 倍成本，更能大大提升工作效率。

现今，应用程序漏洞仍旧是网络安全的首要顾虑。尽管攻击者不断利用新的应用漏洞，研究人员也不断披露，但最常见的应用程序缺陷往往是之前已反复发现的威胁。已知的应用程序漏洞如此之多，一方面表明了许多开发团队未能具备所需的安全能力和资源以应对潜在安全缺陷，另一方面也反映了市场明显缺乏具有足够应用安全知识与技能的合格软件专业人员。 如果不采取有效措施应对这一软肋， 企业与政府机构将不得不

面临并持续遭遇数据泄露、运营中断、业务受困、品牌受损、监管罚单等一系列严重后果。这就是为什么软件从业人员不断更新软件开发知识与技能、紧跟软件开发行业发展趋势与动态、同时了解新兴安全威胁的重要性所在。

CSSLP 证明持证软件从业人员具备将身份验证、授权、审计等最佳安全实践融入软件开发生命周期各个阶段（从软件设计、实施到测试和部署）的专业知识与能力。

（4）IAPP

国际隐私专业协会(IAPP) 成立于 2000 年，是一个非营利组织，致力于在全球范围内帮助定义、促进和改进隐私专业。致力于为隐私专业人士提供了一个共享最佳做法、追踪趋势、推进隐私管理问题、规范隐私专业管理的平台，为信息隐私领域和专业人士提供相关教育和指导。IAPP 提供了一套完整的教育和职业发展服务，包括隐私培训、认证项目、出版物和年会论坛。

CIPP（注册信息隐私专家）

CIPP 是首个信息隐私方面的认证资质，将向世界展示持证人员知道隐私法律和法规以及如何应用它们并且知道如何确保在信息经济中的地位。因各国(地区)数据安全政策不同，CIPP 认证又分为 CIPP/E(Europe)、CIPP/A(Asia)、CIPP/US(U.S. Private-sector)、CIPP/C(Canada)和 CIPP/G(US.Government)等 4 个子类。CIPP 认证主要适用于隐私保护法律法规、合规性审查、信息管理、数据治理、人力资源等领域的从业人员。

CIPM（注册信息隐私管理师）

CIPM 则主要满足隐私项目生命周期内风险管理、隐私运行、审计与追责、隐私分析等方面的需求，主要适用于风险管理、隐私操作、审计、隐私分析、职责划分等相关的从业人员。

CIPT（注册信息隐私技术专家）

CIPT 面向 IT 从业者开展隐私保护认证，可证明专业人员在 IT 产品和服务的开发、工程、部署与审计方面，对于隐私和数据保护实践的理解程度，以及管理和建立隐私保护要求和控制措施的能力，主要适用于信息技术、信息安全、软件工程、隐私设计、合规审计等相关的从业人员。

（5）其他认证

ITIL 4 Foundation 认证

ITIL 4 是在 ITIL V3/2011 基础上开发的新版本，指导广大客户面对数字化时代 IT 服务管理所带来的挑战，并提供一个灵活、协调和集成的系统，以有效地治理和管理 IT 驱动（IT-enabled）的服务。

ISO/IEC27001 网络安全管理

ISO/IEC 27001 (ISO 27001)是信息安全管理的国际标准，提供了建立、实施、维护和持续改进信息安全风险管理系统(ISMS)的体系化运行模式。该标准是有效管理敏感、机密信息和应用信息安全控制的管理模式。

符合 ISO/IEC 27001 标准的组织拥有明确、客观的证据，证明其承诺持续改进对其敏感和机密信息的控制。因此，ISO/IEC 27001 让业主、股东和客户放心，保护企业和相关方的信息系统安全、知识产权、商业秘密等。

ISO 20000 审核员

ISO 20000 是世界上**第一部**针对信息技术服务管理（IT Service Management）领域的国际标准，ISO 20000 信息技术服务管理体系标准代表了被广泛认可的评估 IT 服务管理流程的原则的基础。该标准定义了一套全面的、紧密相关的服务管理流程。

ISO 20000 是面向机构的 IT 服务管理标准，目的是提供建立、实施、运作、监控、评审、维护和改进 IT 服务管理体系(ITSM)的模型。

PMP（项目管理专业人士）

PMP 是项目管理专业人士资格认证，由美国项目管理协会 (简称 PMI®) 发起。PMP 在全球范围内对项目管理人员的职业资格认证，其目的是为了给项目管理人员提供统一的行业标准；作为项目管理资格认证考试，已在国际上树立了其权威性。现中国已有超 43 万人参加 PMP 考试。

EXIN DPO（数据保护官）

随着欧盟 GDPR 法规以及国内网络安全法、首部民法典、个人信息保护法(草案)的出台，隐私作为一种权利，越来越受到个人的重视和国家的监管。做为数据合规从业人员，既要懂隐私保护，又要懂信息安全！

考取该证书不仅意味着成功通过了对欧盟法规的全面考察，更加意味着拥有了在组织中担任实施与维护 GDPR 的能力。

DPO 总共三门课分别为：EXIN PDPF 讲述 GDPR 法律法规；EXIN PDPP 讲述隐私保护管理体系；EXIN ISO27001 Foundation 讲述信息安全基础知识）。

目前全国已有大约 700 多人获得 EXZN DPO 证书，受众群体为凡是涉及到个人信息的企业、或在欧盟设有分支机构及业务的企业及行业等。

4.4.2.2 国内信息安全认证体系

目前国内信息安全认证体系按照国内的发证机构区分，大致可以分为公安部 、中国信息安全产品测评认证中心、国家反计算机入侵和防病毒研究中心、人力资源和社会保障部、工业和信息化部这几大类。

CIIPT（国家重要信息系统保护人员）

公安部信息安全等级保护评估中心（以下简称“评估中心”）是由公安部为建立网络安全等级保护制度，构建国家网络安全保障体系而专门批准成立的专业技术支撑机构。为了更好地服务于等级保护制度的深入开展，满足相关人员的培训需求，评估中心制定和实施了我国重要信息系统安全保护人员培训计划（CIIPT)。

CIIPT(Critical Information Infrastructure Protection Training)，培训的知识体系是以等级保护相关政策法规为指导，以重要信息系统保障为核心，基于等级保护相关岗位技能需求，以等级保护相关标准体系为主线，根据具体岗位工作任务系统化梳理而成的。

我国重要信息系统的规划、设计、建设、运行维护需要大量专业技术人员，根据不同人员的培训需求不同，设置不同的培训课程，目前主要分为针对技术人员的 CIIP-A 和针对管理干部的 CIIP-D 两类证书培训。

国家重保人员认证可以作为企业开展等保测评工作的内审人员的岗位培训。是国内针对等保工作面向非等保测评机构人员较具权威的证书，当前全国有约 10000 人获得该证书。

获得证书人员表明接受过国家网络安全政策、法规和标准的专业培训，掌握和了解我国重要信息系统的规划设计、建设整改、运行维护的相关要求。具备我国重要信息系统保护对相关人员的基本能力要求。

CISP（注册信息安全专业人员）

CISP 即“注册信息安全专家”，是经中国信息安全产品测评认证中心实施国家认证，代表国家对信息安全人员资质的最高认可；是有关信息安全企业，信息安全咨询服务机构、信息安全测评认证机构和授权测评机构、社会各组织、团体、企事业有关信息系统建设、运行和应用管理的技术部门和标准化部门必备的专业岗位人员，其基本职能是对信息系统的安全提供技术保障，全国约有 50000~70000 名获证人员。

根据实际岗位工作需要，CISP 分为三类：CISE 主要从事信息安全技术开发服务工程建设等工作，CISO 从事信息安全管理等相关工作，CISA 从事信息系统的安全性审核或评估等工作。

课程包括了信息安全保障、网络安全监管、信息安全管理、业务连续性、安全工程与运营、信息安全评估、信息安全支撑技术、物理环境与网络通信安全、计算环境安全、软件安全开发知识体系。

目前，国内各大安全专业服务公司都具备相应数量的 CISP 专家。

CISP-PTE（注册信息安全专业人员-渗透测试工程师）

CISP-PTE（注册信息安全专业人员-渗透测试工程师）由中国信息安全测评中心颁发，此证书专注于培养考核高级应用安全人才，是业界首个理论与实践相结合的技能水平注册考试，是国内认可度极高的渗透测试认证，其专业性强，技能要求高。CISP-PTE 对申请人员无工作经验和学历的要求。目前全国已有大约 3000 多人获得 CISP-PTE 证书。

注册信息安全专业人员-渗透测试是为了锻炼考生实际解决网络安全问题的能力，有效增强我国网络安全防御能力，促进国家企事业单位网络防御能力不断提高，以发现人才，选拔优秀人才而设立的技能水平考试，证书持有人员主要从事信息安全技术领域

网站渗透测试工作，具有规划测试方案编写项目测试计划、编写测试用例、测试报告的基本知识和能力。

CISP-DSG（注册数据安全治理专业人员）

CISP-DSG 即“注册数据安全治理专业人员”，是中国信息安全测评中心联合天融信开发的针对数据安全人才的培养认证，是业界首个针对数据安全治理方向的国家级认证培训。

证书持有人员主要从事数据安全治理相关工作，具有数据安全治理过程管理、数据安全技术体系设计、数据安全管理体系设计的基本知识和能力。目前全国已有大约 500 多人获得 CISP-DSG 证书。

CISP-DSG 知识体系包括信息安全保障、信息安全评估、网络安全监管、信息安全管理、数据安全基础知识、数据安全技术体系、数据安全管理体系这四个知识类，每个知识类根据其逻辑划分为多个知识体，每个知识体包含多个知识域，每个知识域由一个或多个知识子域组成。

CISAW（信息安全保障**人员认证**）

CISAW 是中国信息安全认证中心历经六年，集业界专家、企业精英、高校及研究机构学者参与打磨的针对信息安全保障不同专业技术方向、应用领域和保障岗位，依据国际标准 ISO/IEC17024《人员认证机构通用要求》所建立的、不同层次的信息安全保障人员认证体系。

CISAW 经过全新改版，针对技术专业和应用领域，建立了安全集成、安全运维 风险管理 、应急服务、安全软件、工控网络安全、能源行业工业控制系统网络安全、电子数据取证、网络舆情分析与处置、WEB 安全、CA 服务、渗透测试的认证方向，针对不同的层次，不同专业的信息安全岗位，为信息安全从业人员提供了较为完整的一套认证体系。

考取 CISAW 不同认证方向，有具体的学历要求及工作经验。

CSAO（注册信息安全意识官）

CSAO 即注册信息安全意识官，由 CEAC(The Cyberspace Security Talent Education Alliance of China，中国网络空间安全人才教育论坛)颁发认证。认证课程是国内首个“人为因素”安全风险管理专业认证课程，旨在面向政企事业单位负责安全文化建设、管理内部“人为因素”风险以及实施安全意识宣导的专/兼职人员，提供全方位的方法论与实践指导，并将“人为因素”风险管理工作进行体系化、可视化和可度量，以提升企业安全意识成熟度水平，更有效满足合规要求及降低“人为因素”风险。

企业可通过开展 CSAO 认证培训，为组织内部培养专业的专/兼职岗位安全教育志愿者，帮助组织快速建立各级安全宣传工作队伍，通过科学的工作方法与知识工具，有效连接带动身边每位员工，共同关注身边的信息安全，形成企业安全文化。目前全国已有大约 360 多人获得 CSAO 证书。

CCSS-M（网络安全服务能力认证—安全管理能力认证）

网络安全服务能力认证—安全管理能力认证(简称 CCSS-M)由国家反计算机入侵和防病毒研究中心负责。该组织由科技部、公安部批准，在上海市政府支持下，由公安部第三研究所负责组建，是进行信息安全领域反计算机入侵和防病毒研究及成果产业化的国家级研究基地。发证机构为国家反计算机入侵和防病毒研究中心（公安部第三研究所）。

本认证目的在于培训、考核各单位安全管理人员在安全岗位人员角色定位、安全职责内容分配、日常安全工作协调、日常信息安全规范管理等方面的统筹协调能力，以及对于专项安全行动支持、网络安全工作、事件通报及预警处置管理、网络安全法律法规解读等方面采取措施及统筹能力。证书目标人群为单位及企业的安全部门管理者；有意向从事安全管理者工作人员。

ITSS(服务项目经理和服务工程师）

IT 服务工程师培训”和“IT 服务项目经理培训”是中国电子技术标准化研究院推出的 ITSS 系列培训，通过该培训的人员可系统掌握 IT 运维的知识，提升项目管理水平，有效满足 GB/T 28827.1 的符合性评估要求。中国电子技术标准化研究院软件应用与服务研究中心组织开展 ITSS 系列培训工作。

ITSS 能提高企事业单位的 IT 服务管理水平，规范 IT 服务的行为，降低 IT 运营的风险，保障业务正常、稳定、高效的运行，增加 IT 投资的回报率；通过 ITSS 系列培训，可以培养从业人员熟练掌握 ITSS 内容，提升 IT 运维服务能力；企事业单位可以在 ITSS 标准的指导下开展 IT 服务工作。推动信息技术标准 ITSS 在 IT 服务行业的广泛应用。

信息系统项目管理师

信息系统项目管理师属于计算机技术与软件（高级）专业技术资格。

通过本考试的合格人员能够掌握信息系统项目管理的知识体系，具备管理大型、复杂信息系统项目和多项目的经验和能力；根据需求组织制订可行的项目管理计划；能分析和评估项目管理计划和成果；能在项目进展的早期发现问题，并有预防问题的措施；能协调信息系统项目所涉及的相关人员；具有高级工程师的实际工作能力和业务水平。颁发证书单位是工信部和人社部。

信息网络安全专业人员(INSPC)认证

本证书颁发机构为公安部国家反计算机入侵和防病毒研究中心。

认证目标是让持证人员掌握信息安全和管理所必需的基础理论知识，掌握信息系统的基本安全管理、评估和基础防御技术，掌握主流网络和信息安全产品的基础配置管理，并能有效提高互联网用户防范日益增多的网络盗窃和入侵的能力，有效保护个人及单位的资金账户和重要信息。

第五章 数字安全评价层

5.1 数字安全奖项与排行

5.1.1 数字安全企业评估参考

业界存在众多安全相关的奖项及业界大会，这些大会及奖项目的除了通过大会协助全球认识到安全面对的威胁，同时也介绍新的防护技术，并表扬领域上的杰出企业、方案、产品、及优秀人士。下面是国内外具有代表性的大会及相关奖项。

5.1.1.1 云安全联盟大中华区

云安全联盟大中华区是在香港正式注册的独立、中立、权威性非营利组织，是国际云安全联盟 CSA 的全球四大区之一(其它大区为美洲区、亚太区、欧非区)。云安全联盟大中华区创立中国神兽方阵模型（China Matrix Quadrant），方阵接受联合国科学技术促进发展委员会和联合国数字安全联盟指导，秉着中立公正、专业权威的原则，相关数据将作为联合国全球数字安全报告内容的重要参考。

云安全联盟大中华区对中国企业在数字安全的各子领域进行分析、展示、排行。在方阵中，各神兽可以代表中国的独角兽企业，也可以代表更强大的先进企业，以及在创业成长期中有潜力成为未来独角兽的创新企业，为数字经济和数字安全产业的高质量发展提供参考和借鉴。

云安全联盟大中华区发布的神兽方阵系列包括云安全、数据安全、零信任、区

块链安全、物联网安全、隐私科技等数字技术安全领域，这个模型从对企业从技术先进性与市场影响力两个维度进行评估，在研发能力、知识产权、产品成熟度、营收情况、签约情况、营销情况等六个打分项做出分析与评价，每年度对方阵进行更新，由中国网、中国科技新闻网等官方媒体传播给全球读者与广大客户群体。首先推出的零信任神兽方阵于 2022 年发布[23]。

5.1.1.2 中国网络安全产业联盟（CCIA）

联盟是由积极投身于网络安全产业发展，开展网络安全理论研究、技术研发、产品研制、测评认证、教育培训、安全服务等相关业务的企事业单位以及用户单位自愿组成，属于全国性非营利行业组织，旨在营造良好的网络安全产业发展环境，

[23] https://c-csa.cn/research/results-detail/i-1864/

保障中国国家网络安全和用户利益，推动网络安全产业做大做强。

网络安全解决方案优秀奖

致力于推选我国网络安全产业优秀创新成果，激发网络安全企业加强自主创新能力，搭建网络安全企业、技术、人才和资本合作的平台，推动网络安全产业高质量发展。2018 年 8 月首次发布，是 CCIA 最早的评选奖项之一，每年在中国网络安全周期间发布，评委团由网络安全主管部门、行业用户、投融资机构、高等院校、科研机构的 10 位点评专家和 50 位观众评委共同组成，是国内重要的网络安全奖项之一。

中国网络安全市场竞争力报告

报告主要针对国内安全领域总体发展进行统计和分析，同时针对热点板块进行拆分整理和评估，有比较客观的参考意义。

中国网安产业竞争力 50 强（CCIA 50 强）

评选主要从“资源力”和“竞争力”两个维度对企业综合能力进行画像。2020 年进行首次评选，每年 6 月在其官网上发布，各大安全网站、媒体都会以各种形式转载。

中国网安产业成长之星（CCIA 成长之星）

榜单的评选目标是通过数据分析，发现网络安全行业中聚焦新兴的安全细分市场，在竞争中处于优势地位，具备进一步高速成长的创新型企业。该榜单的评选主要面向商业模式相对成熟，未来业务重点和经营策略确定的企业，从企业竞争力（品牌、营销、产品、研发、服务和经营）、企业成长周期、企业成长性及安全是否为主营业务等方面进行多维度考评，最终确定榜单。成长之星首次发布在 2020 年月，之后每年 6 月与 CCIA 年度多项榜单同期发布。

中国网安产业潜力之星（CCIA 潜力之星）

中国网安产业潜力之星备选企业是 B 轮以前或成立 5 年以内的企业。评价指标主要以企业竞争力（品牌、营销、产品、研发、服务和经营）为基础，结合企业成长速度、成长性、资本市场关注度等维度的数据计算得出，企业从事业务方向创新性强也是重要的参考维度。CCIA 潜力之星首次发布在 2020 年月，之后每年 6 月与 CCIA 年度多项榜单同期发布。

5.1.1.3 安全牛

安全牛是中国网络安全领域的专业媒体和旗舰智库，精确定位并服务于

CISO/CSO/CTO/CIO 决策者人群，向国内企业的决策管理者以及 IT 专业人士提供独立客观、高品质、有价值的战略性网络安全内容。安全牛致力于推动中国企业跨越“安全鸿沟”，促进中国网络安全产业的健康发展。

中国网络安全行业全景图

总结行业的全景图，可以方便关注领域的人士快速查阅、参考、分享和传播。2016 年 9 月，安全牛团队基于对我国安全行业的调研和积累，结合网络安全厂商产品信息申报，首次推出中国网络安全行业全景图，对我国网络安全产业整体发展状况及细分领域代表性厂商进行展现，受到行业广泛关注。2020 年之后评估日趋趋成熟，2022 年第九版“全景图”包含 14 项一级安全分类，94 项二级安全分类.

中国网络安全企业 100 强

安全牛于 2015 年 7 月，在行业中率先发起全国性网络安全厂商调查活动，并推出第一版《中国网络安全企业 50 强》报告，受到行业广泛关注。随着我国网络安全产业快速发展，原“50 强”报告于 2019 年 7 月经调研扩增至“100 强”并延续至今。2021 年 11 月 9 日，第九版中国网络安全企业 100 强（基于 2020 年度数据）正式发布。

5.1.1.4 Freebuf

FreeBuf 是国内领先的网络安全行业门户，同时也是爱好者们交流与分享安全技术的社区。

CCSIP 中国网络安全产业全景图

随着全社会数智化转型的起步，网络安全领域加速迭代，整体发展更具规模化、产业化、集群化。同时，受益于国家政策推动，全行业持续高景气发展。面对网络安全的新形势，FreeBuf 咨询始终紧跟网络安全市场发展趋势，关注企业发展现状、跟踪前沿技术，确保 CCSIP 全景图对业内人士的长期参考价值，自 2018 年开始，每年不定期发布“中国网络安全产业全景图”。全景图与安全牛“**中国网络安全行业全景图**”相比，偏重于产品和技术方面的综合能力评估，同时在细分领域上也和其它主流安全评估略有差异。

网络安全创新大会

2015 年底，FreeBuf 主办了 2015 WitAwards 年度互联网安全评选，并在 2016 年初首次举办年度互联网安全创新大会（FIT），之后每年年底或者年初定举行。2019 年，大会更名为“CIS 网络安全创新大会”，每期大会都会有不同的主题和侧重，旨在

将最新的网络安全战略、话题、技术、方案等集中发布。

Wit Awards 中国网络安全行业年度奖项包括：

- 年度安全作者
- 年度热门安全产品与服务
- 年度安全品牌影响力
- 年度安全 SRC
- 年度产业领军企业
- 年度创新产品
- 年度技术变革
- 年度优秀解决方案

5.1.1.5 IDC

IDC 成立于 1964 年，是全球领先的科技媒体、数据和营销服务公司 International Data Group (IDG, Inc.)的全资子公司。在安全方面，每年 IDC 会召开多个全球性会议，并在每年公布以下奖项：

- IDC 年度全球 CSO 网络安全大会
- CSO 20 Awards: 中国 20 大杰出安全项目
- CSO HALL of FAME（全球 CSO 名人堂）及中国 CSO 名人堂（十大人物）

IDC 年度全球 CSO 网络安全大会自 2015 年举办至今已在全球超过 10 个国家和地区成功举行，2020 年的美国峰会吸引了超过 1000 位 CIO 和 CSO 参与，线上直播观众超过 15 万人次。2022 年大会由 Foundry（IDG）/IDC 联合上海市网络安全协会共同举办，为表彰安全领域的杰出项目及人物，本届大会首度设立“中国 20 大杰出安全项目” 和“中国 CSO 名人堂（十大人物）”奖项评选。

5.1.1.6 Business Intelligence Group

Fortress Cyber Security Award

Fortress Cyber Security Award 是由 Business Intelligence Group 组织的一系列网络安全相关的奖项。

Business Intelligence Group 的目标是寻找并奖励那些具有远见、创造力和毅力的人，而这些奖项都是在全球领先的公司和个人的一个标志。该组织自 2012 年以来，已经表彰并奖励了数百名企业高管、部门、产品。目的是突出和奖励那些在全球网络安全日益严重的威胁下，提出创造性思维、工程、人员和项目。

Fortress Cyber Security Award 奖项类别包括：

- 分析（ANALYTICS）
- 应用安全（APPLICATION SECURITY）
- 身份验证和身份（AUTHENTICATION & IDENTITY）
- 区块链（BLOCKCHAIN）
- 合规（COMPLIANCE）
- 密码学（CRYPTOGRAPHY）
- 数据保护（DATA PROTECTION）
- 加密（ENCRYPTION）
- 端点检测（ENDPOINT DETECTION）
- 事件响应（INCIDENT RESPONSE）
- 网络安全（NETWORK SECURITY）
- 威胁检测（THREAT DETECTION）
- 培训（TRAINING）
- 卓越组织（ORGANIZATIONAL EXCELLENCE）
- 领导力（LEADERSHIP）

5.1.1.7 Cyber Defense Media Group

网络防御媒体集团（Cyber Defense Media Group）是世界上领先的网络防御新闻和信息平台，于 2012 年 1 月开始在全球帮助信息安全创新者传播信息并扩大规模。同时，网络防御媒体集团非常关心网络防御，并建立各网络防御平台，其中又以网络防御奖最为著名。

网络防御全球信息安全奖自 2012 年以来要求参与者必须有创新的网络安全产品、服务或解决方案供评委审核，每年的网络防御全球信息安全奖与 RSA Conference 或其母公司 Dell 无关，也不由其拥有或运营。 奖项包括：

- 前 10 黑色独角兽
- 前 10 新生黑色独角兽
- 前 10 网络安全初创公司
- 前 10 MSSP
- 前 10 网络安全女性
- 前 10 网络安全专家
- 前 10 首席信息安全官

5.1.1.8 Gartner

Gartner 公司成立于 1979 年，是第一家信息技术研究和分析的公司,为有需要的技术用户提供专门的服务。Gartner 已经成为了一家独立的咨询公司，Gartner 公司的服务主要是迎合中型公司的需要，希望使自己的业务覆盖到 IT 行业的所有领域，从而让自己成为每一位用户的一站式信息技术服务公司。

魔力象限

Gartner 魔力象限是监测和评估专业科技市场中公司发展及定位的一种研究方法论和形象化工具。对于有意向找一家能满足自身需求的公司的投资者以及力图在市场中赢得竞争并获得优势的企业，魔力象限研究报告用处极大。

与单纯的给出统计数字或者列表为公司排名不同，魔力象限使用二维模型阐释公司间的实力及差异。魔力象限基于公司发展前景的完备性和执行能力，将构成竞争的公司分成四个不同的部分。

- 利基型企业(也称利益市场、小众市场)
- 有远见者
- 挑战者
- 行业领袖

魔力象限由 Gartner 公司于 2006 年提出，并没有特别区分网络安全及其他的行业，排名都可以在 Gartner 的网站查看，关于网络安全方面相关的排名主要有以下：

- 访问管理
- 应用安全测试
- 云访问安全代理
- 端点保护平台
- 企业网络防火墙
- 入侵检测和防御系统
- IT 风险管理
- 托管网络服务
- 特权访问管理
- 安全 Web 网关
- 基于计算机的安全意识培训
- 安全信息和事件管理

- 安全服务边缘
- Web 应用程序和 API 保护
- Web 应用程序防火墙

5.2 数字安全认证

当今世界已进入数字时代，数据成为国家基础性战略资源、重要生产要素。全球数据爆发增长，海量集聚，成为实现创新发展、重塑人们生活的重要力量，事关各国安全与经济社会发展。数字安全对于推动经济高质量发展，助力国家治理体系和治理能力现代化具有重要作用。近年来针对数据的攻击、窃取、劫持、滥用等手段不断推陈出新，社会、经济、科技、民生等领域面临巨大潜在风险。

为切实保障数字安全，国际社会各方在实践中不断探索。数字安全认证已逐渐成为全球数据治理的重要手段。数据安全认证本质上是第三方提供的服务，承担着第三方规制的角色。构建法治化的数字安全认证体制机制，不仅有利于保障数据安全，而且可以有效促进数字经济的规范健康发展。

数字安全认证是指由认证机构证明产品、服务、组织等符合相关法律规范、技术标准的评定活动。数字安全认证主要通过第三方认证机构按照相关安全标准，客观评定数据处理行为的安全性。

5.2.1 产品测评认证

随着科学技术日新月异的提升迭代以及互联网的高速发展，世界正在进入以信息产业为主导的快速发展时期。信息技术已经被广泛应用在各行业中，有效推动社会进步与经济发展。信息安全产品和信息系统因其特有的敏感性和特殊性，对社会秩序、经济建设、公众利益、乃至国家安全均构成直接或间接的深远影响。

产品评测认证依据国家标准 GB/T 18336—2015《信息安全技术 信息技术安全评估准则》以及其他信息技术产品测评标准，综合考虑产品的构成要素和应用环境，通过对信息技术产品的整个生命周期 (包括研制、开发、管理、交付、使用等) 进行全面的评估和测试，验证产品的保密性、完整性、可用性和安全性程度，确定产品是否满足相关评测标准的要求, 为最终用户判断产品提供决策依据和权威公正的专业指导。

产品评测主要是由测评机构按照相关标准对产品进行测评，达到测评要求后，出具产品认证证书。目前，国内产品测评机构主要有国家保密科技测评中心、中国信息安全认证中心、国家网络与信息系统安全产品质量监督检验中心、公安部计算机信息系统安全产品质量监督检验中心、国家密码管理局商用密码检测中心等。

5.2.1.1 目的和意义

产品评测认证是产品安全质量、产品安全使用的重要保障措施，其目的是促进高质量、安全和可控的产品的开发。产品评测具体的目的和意义主要包括:

- 排除产品的安全隐患，确保产品质量;
- 帮助用户选择安全可靠的产品，让用户使用更加放心;
- 助力企业建立健全有效的管理监督体系，进一步提升产品质量;
- 严格规范和科学引导企业的研制、开发、生产、使用等，提高其市场竞争力和技术研发水平，使企业发展进入良性循环;
- 有助于在涉及国家安全的信息安全领域中加强产品和服务的安全性和可控性，维护用户的安全利益，确保产品符合国家安全标准;
- 促进信息技术产业的稳步持续发展，提升信息技术产业成熟度，推进信息技术产品市场规范化、标准化建设;
- 助力企业加强自主创新和保护知识产权的意识，提高企业产品和服务的自主创新能力和水平。

5.2.1.2 业界主要标准和指南

相关的评测标准主要有：GB(国家标准），QB(行业标准），DB(地方标准)，企业标准，国际标准等。

5.2.1.2.1 国家标准

国家标准是指由国家机构通过并公开发布的标准，包括强制性国标（GB）和推荐性国标（GB/T）。业界标准有：

- GB/T 20272-2019《信息安全技术 操作系统安全技术要求》
- GB/T 20275-2013《信息安全技术 网络入侵检测系统技术要求和测试评价方法》
- GB/T 20279-2015《信息安全技术 网络和终端隔离产品安全技术要求》
- GB/T 18336-2001《信息安全技术 信息技术安全性评估准则》
- GB/T 20281-2015《信息安全技术 防火墙安全技术要求和测试评价方法》
- GB/T 21028-2007《服务器安全技术要求》
- GB 17859-1999《计算机信息系统安全保护等级划分准则》
- GB/T 22186-2016《信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求》等。

5.2.1.2.2 行业标准

行业标准是对国家标准的补充，是在全国范围的某一行业内统一的标准。业界标准有：

- YD/T 4065-2022《移动终端可信环境安全评估方法》
- YD/T 4060-2022《云计算安全责任共担模型》
- YD/T 4041-2022《智慧城市 电子围网技术要求》
- YD/T 4029-2022《计算存储分离架构的分布式存储技术要求》
- YD/T 4025-2022《互联网边缘数据中心术语》
- 云安全联盟联合公安部第三研究所和业界专家制定的《云应用安全标准》
- 云安全联盟联合公安部第三研究所和业界专家制定的《云原生安全标准》等。

5.2.1.2.3 地方标准

地方标准由省、自治区、直辖市人民政府标准化行政主管部门编制计划，组织草拟，统一审批、编号、发布，并报国务院标准化行政主管部门和国务院有关行政主管部门备案。业界标准有：

- DB11/T 1961-2022《软件和信息化项目运行评价指标体系》
- DB11/T 932-2021《数字化城市管理信息系统部件和事件处置》
- DB11/T 310-2021《数字化城市管理信息系统技术要求》
- DB31/T 1083-2018《公共停车信息联网技术要求》
- DB35/T 2018-2021《信息化业务协同标准符合性测试》等。

5.2.1.2.4 企业标准

企业标准是对企业范围内需要协调、统一的技术要求、管理要求和工作要求所制定的标准。业界标准有：

- 《5G 国密物联网卡 HTTP 设计技术》
- 《车载智能信息终端》
- 《华为数据中心存储阵列》
- 《华为 HarmonyOS 生态链的智能跑步机》等。

5.2.1.2.5 国际标准

国际标准由国际标准化组织（ISO）、国际电工委员会（IEC）、国际电信联盟（ITU）制定的标准，或经国际标准化组织（ISO）确认并公布的其他国际组织制定的标准。业

界标准有：

- ISO/IEC 27070:2021 《 Information technology — Security techniques — Requirements for establishing virtualized roots of trust》
- ISO/IEC 27036-3:2013《Information technology — Security techniques》
- ISO/IEC 19987:2017 《 Information technology — EPC Information Services (EPCIS) Standard》
- ISO/IEC 23681:2019 《 Information technology — Self-contained Information Retention Format (SIRF) Specification》
- ISO/IEC 5230:2020《Information technology — OpenChain Specification》等。

5.2.1.3 典型认证类型

根据认证对象和认证要素的不同，产品评测认证主要包括产品型式认证、产品认证、信息系统安全认证、信息安全服务认证。

根据测评依据及测评内容，产品评测认证包括产品分级评估、产品认定测评、产品自主原创测评、源代码安全风险评估、安全渗透、信息系统攻击测试、选型测试、定制测试等。

根据产品安全性进行测评，测评内容包括防火墙、安全审计、网络隔离、VPN、智能卡、安全管理、安全设备、入侵检测、入侵防御、WAF、上网行为管理、漏洞检测和扫描设备、反病毒、移动安全、终端安全、云安全等；以及非安全专用产品，包括操作系统、数据库、交换机、路由器、应用软件等。

根据所属业务的不同，包括基础硬件、基础软件、存储备份、外设、多媒体、日常办公、业务系统、安全防护、设计开发等相关产品认证。

根据所属领域的不同，包括物理安全、网络安全、数据安全、用户安全、管理安全、平台安全、身份鉴别与访问控制安全、移动安全等相关产品认证。

5.2.1.3.1 物理安全认证

物理安全认证主要包括对计算机电磁干扰器、低泄射信息设备、网络隔离传导干扰装置、防线路截获、载体检测门禁、计算机网络传导干扰器、保密柜、载体在位监测、智能卡、终端、存储、安全设备、网络设备、服务器等产品进行安全认证。其认证类型包括：3C 认证，CQC 认证，CE 认证，FCC 认证等。

5.2.1.3.2 网络安全认证

网络安全认证主要包括对网络终端接入控制系统、防火墙、安全网关、网络隔离、

远程访问安全、入侵防范、入侵检测、安全协议、安全网络设备、安全服务器、安全终端等进行安全认证。其认证类型包括：《网络关键设备和网络安全专用产品安全认证》《国家信息安全产品认证》《ICSA Labs》等。

5.2.1.3.3 数据安全认证

数据安全认证主要包括对存储数据保护、数据备份与恢复、数据防篡改、数据防泄露、数据擦除等进行安全认证。其认证类型包括：《数据安全管理认证》等。

5.2.1.3.4 用户安全认证

用户安全认证主要包括对身份鉴别与访问控制、防御恶意程序、可信授权认证、桌面主动防御、安全办公软件、证书授权认证、标签水印等进行安全认证。其认证类型包括：《信息安全保障人员认证》《网络安全应急响应工程师认证》等。

5.2.1.3.5 管理安全认证

管理安全认证主要包括对网络审计监控、终端审计监控、脆弱性检测、威胁与分析、安全检查、网络安全管理、日志分析与审计、终端安全管理、介质安全管理、安全配置管理等进行安全认证。其认证类型包括：《信息安全管理体系认证》《信息安全服务资质认证》《信息技术—服务管理体系认证》等。

5.2.1.3.6 平台安全认证

平台安全认证主要包括对操作系统安全、数据库安全、虚拟化平台安全、云计算、物联网平台安全、工控平台安全、大数据平台安全、人工智能平台安全、可信计算平台安全等进行安全认证。其认证类型包括：《云计算服务安全评估》《大数据产品能力认证》《云安全评估认证（C-STAR）》等。

5.2.1.3.7 身份鉴别与访问控制安全认证

身份鉴别与访问控制安全认证主要包括对生物特征认证、IC 卡认证、终端认证、PKI(CA)认证、数字签名认证、数字印章认证、数字水印认证、视觉监控等进行安全认证。其认证类型包括：CCRC 认证、《ISO 27018 公有云个人可识别信息安全管理体系认证》等。

5.2.1.3.8 移动安全认证

移动安全认证主要包括对移动智能终端应用软件、移动智能终端操作系统、3G/4G/5G 相关软硬件产品进行安全认证。其认证类型包括:《移动互联网应用程序（App）安全认证》《移动金融技术服务认证》等。

5.2.1.3.9 其他

其他认证包括工控产品认证、物联网终端产品认证、云计算安全防护产品认证、评估保障级产品认证、智能卡产品认证、商用密码产品认证以及其它 IT 产品认证，认证类型包括《云应用安全认证》《云原生安全认证》等。

5.2.2 服务安全认证

数字安全服务是安全服务提供方提供安全服务的一种能力，包括法律地位、资源状况、管理水平、技术能力等方面的要求。

服务安全认证对提供安全服务的组织和单位资质进行审核、评估和认定。包括对安全服务提供者的技术、资源、法律、管理等方面的资质和能力，以及稳定性、可靠性等进行评估，并依据公开的标准和规范对其安全服务保障能力进行认定的过程。

5.2.2.1 目的和意义

安全服务认证是依据国家法律法规、国家标准、行业标准和技术规范，按照认证基本规范及认证规则，对提供信息安全服务提供方的信息安全服务能力进行评价。通过对安全服务的资质认证，

- 可以对信息安全服务提供商的基本资格、管理能力、技术能力和服务过程能力等方面进行权威、客观、公正
- 认证过程能有效促进服务提供商完善自身管理体系，提高服务质量和水平的评价，证明其服务能力，满足社会对服务的选择需求。

5.2.2.2 业界主要标准和指南

业界主要的标准和指南有：

- 《信息系统安全集成服务资质认证评价要求》RB/T 201-2013
- 《网络与信息安全应急处理服务资质评估方法》（YD/T 1799-2008）
- 《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）
- 《信息安全技术 重要工业控制系统网络安全防护导则》（GB/Z 41288-2022）
- 《信息安全技术　信息系统安全运维管理指南》（GB/T 36626-2018）
- 《信息安全技术　应用软件安全编程指南》（GB/T 38674-2020）
- 《信息安全技术　灾难恢复服务能力评估准则》（GB/T 37046-2018）

5.2.2.3 典型认证类型

安全服务认证主要包含安全集成、风险评估、安全运维、应急处理、软件安全开发、

灾难备份与恢复、网络安全审计、工控安全、云安全等服务认证。

5.2.2.3.1 安全集成服务认证

安全集成服务是指从事计算机应用系统工程和网络系统工程的安全需求界定、安全设计、建设实施、安全保证的活动。安全集成包括在新建信息系统的结构化设计中考虑信息安全因素，从而使建设完成后的信息系统满足建设方或使用方的安全需求而开展的活动。也包括在已有信息系统的基础上额外增加信息安全子系统或信息安全设备等，通常被称为安全优化或安全加固。其认证类型包括：中国网络安全审查技术与认证中心（CCRC）的《安全集成服务资质认证》《ISO27017 云服务信息安全管理体系认证》等。

5.2.2.3.2 风险评估服务认证

风险评估是数据安全保障的基础性工作和重要环节，贯穿于网络和信息系统建设运行的全过程。服务提供者通过对信息系统提供风险评估服务，系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和安全整改措施，防范和消除信息安全风险，或将风险控制在可接受的水平，为网络和信息安全保障提供科学依据。其认证类型包括：中国网络安全审查技术与认证中心（CCRC）的《风险评估服务资质认证》、澳大利亚的信息安全注册评估员计划 (IRAP) 等。

5.2.2.3.3 安全运维服务认证

安全运维服务是通过技术设施安全评估，技术设施安全加固，安全漏洞补丁通告、安全事件响应以及安全运维咨询，协助组织的信息系统管理人员进行信息系统的安全运维工作，以发现并修复信息系统中所存在的安全隐患，降低安全隐患被非法利用的可能性，并在安全隐患被非法利用后及时加以处理。其认证类型包括：等级保护测评等。

5.2.2.3.4 应急处理服务认证

应急处理服务是通过制定应急计划使得影响网络与信息系统安全的安全事件能够得到及时响应，并在安全事件一旦发生后进行标识、记录、分类和处理，直到受影响的业务恢复正常运行的过程。其认证类型包括：CNCERT 的《网络与信息安全应急 CCSRP 认证》等。

5.2.2.3.5 软件安全开发服务认证

软件安全开发服务是通过对软件开发过程的安全控制，将开发的软件存在的风险控制在可接受的水平。软件安全开发服务认证是对软件开发方的基本资格、管理能力、技术能力和软件安全过程能力等方面进行评价。其认证类型包括：《ISO 27034 安全软件

程序流程框架标准》。

5.2.2.3.6 灾难备份与恢复服务认证

灾难备份与恢复服务是将信息系统的数据、数据处理系统、网络系统、基础设施、专业技术支持能力和运行管理能力进行备份，并在灾难发生时，将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计和提供的活动。其认证类型包括：可信云的《云容灾解决方案能力评估认证》等。

5.2.2.3.7 网络安全审计服务认证

网络安全审计是指网络安全审计机构对被审计方所属的计算机信息系统的安全性、可靠性和经济性进行检查、监督，通过获取审计证据并对其进行客观评价所开展的系统的、独立的、形成文件的活动。其认证类型包括：《SOC 审计认证》《WebTrust 国际安全审计认证》等。

5.2.2.3.8 工控安全服务认证

工控安全服务围绕提升工业控制系统的高可用性和业务连续性，提升功能安全、物理安全和信息安全的保障能力为目标，涉及工业控制系统设计、建设、运维和技改各个阶段，主要包括系统集成、系统运维、应急处理、风险评估等工业控制系统安全服务，形成系统的、独立的、形成文件的过程。其认证类型包括：《信息安全保障人员（CISAW）能源行业工业控制系统网络安全方向认证》

5.2.3 组织安全认证

5.2.3.1 目的和意义

数字安全是组织可持续发展的基石，近年来国际社会和各国政府都致力于建立和维护开放、透明、公平的数字社会秩序，在这样的背景下，越来越多的组织开始关注其面临的数字安全合规风险以及如何实现数字安全。通过对企业内部进行安全认证：

- 可以向权威机构表明，组织遵守了所有适用的法律法规。从而保护企业和相关方的信息系统安全、知识产权、商业秘密等；
- 可以帮助组织核心业务所赖以持续的各项信息资产进行妥善保护，并且建立有效的业务连续性计划框架，提升组织的核心竞争力。
- 有效保证企业在信息安全领域的可靠性，降低企业泄密风险，更好的保存核心数据；
- 可以强化员工的信息安全意识，规范组织信息安全行为，减少人为原因造

成的不必要的损失。

- 可以证明组织在各个层面的安全保护上都付出了卓有成效的努力，表明管理层履行了相关责任。

5.2.3.2 业界主要标准和指南

- ISO 27001 信息安全管理体系—要求 ISMS Requirements (以 BS 7799-2 为基础)
- ISO 27002 信息技术—安全技术—信息安全管理实践规范 (ISO/IEC 17799:2005)
- ISO 27003 信息安全管理体系—实施指南 ISMS Implementation guidelines
- ISO 27004 信息安全管理体系—指标与测量 ISMS Metrics and measurement
- ISO 27005 信息安全管理体系—风险管理 ISMS Risk management
- ISO 27006 信息安全管理体系—认证机构的认可要求 ISMS Requirements for the accreditation of bodies providing certification
- ISO 27007 信息技术-安全技术-信息安全管理体系审核员指南 Information technology-Security techniques-ISMS auditor guidelines
- ISO 22301 业务连续性管理体系-Business Continuity Management System

5.2.3.3 典型认证类型

5.2.3.3.1 云安全联盟 CSA 的 STAR 认证

云安全联盟 CSA 是在 2009 年的 RSA 大会上宣布成立的。云安全联盟作为业界权威组织，致力于在云计算环境下为业界提供最佳安全解决方案。商业标准公司 BSI （英国标准协会）与云安全联盟强强联手推出 STAR 认证，致力于帮助企业在日趋激烈的云服务市场竞争中脱颖而出。

STAR 认证是信息安全管理体系认证（ISO/IEC 27001）的增强版本，旨在应对与云安全相关的特定问题。2013 年 9 月 26 日，两机构正式宣布推出 STAR 认证项目，该项目采用中立性认证技术对云服务供应商安全性开展缜密的第三方独立评估，并充分运用 ISO/IEC 27001:2005 管理体系标准以及 CSA 云控制矩阵，帮助企业满足对安全性有特定要求的客户需求。

5.2.3.3.2 云安全联盟 CSA 的 CAST 认证

Cloud Application Security Trust（云应用安全可信认证，简称“CAST 认证”）由国际云安全联盟 CSA 大中华区与“公安部第三研究所安全防范与信息安全产品及系统检验实验室”联合发布，是针对 SaaS 产品、在线订阅服务类、IaaS/PaaS 云的应用部分等的安

全可信认证。

CAST 聚焦云应用领域，坚持安全技术与安全合规并重，渗透测试与管理评估并举的原则，致力于提升云应用类产品的安全能力与合规水平，增强客户对云应用类产品安全的信任。

5.2.3.3.3 ISO 27701 隐私信息管理体系认证

ISO/IEC 27701 是对 ISO/IEC 27001 信息安全管理和 ISO/IEC 27002 安全控制的隐私扩展。它是一项国际管理系统标准体系，为保护个人隐私提供指导，包括组织应如何管理个人信息，并协助证明遵守了世界各地的隐私法规。ISO/IEC 27701 的目标是通过对隐私保护的控制对 ISMS 进行补充，有效协助组织对隐私风险进行识别、分析、采取措施，将风险降到可接受水平并维持该水平，最终帮助组织建立完善的个人信息管理体系（PIMS），实现有效的隐私管理。而通过明确对个人验证信息（PII）控制者和处理者的隐私保护要求，可以让组织明确隐私保护管理合规目标，确保组织高级管理层、组织所有者以及关键相关方的利益满足隐私保护要求，从而使组织实现长期的个人隐私安全合规。

5.2.3.3.4 美国国家标准与技术研究院的网络安全框架认证

美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）直属美国商务部，从事物理、生物和工程方面的基础和应用研究，以及测量技术和测试方法方面的研究，提供标准、标准参考数据及有关服务，在国际上享有很高的声誉。

NIST 网络安全框架（ Cybersecurity Framework，CSF）由美国国家标准技术研究所根据《网络安全增强法案》和行政命令 EO13636 “改进关键基础设施网络安全”制定，该框架侧重于使用业务驱动因素来指导网络安全活动，并将网络安全风险视为组织风险管理流程的一部分，使组织可以根据业务和组织需求以具有成本效益的方式解决和管理网络安全风险。NIST CSF 帮助组织根据其业务、任务要求、风险承受能力和资源调整其网络安全活动并确定其优先级，组织可以通过应用该框架的风险管理的原则和最佳实践来提高安全性和弹性。

NIST CSF 由核心要求、实施成熟度和实践指南三大部分组成，并覆盖识别、保护、检测、响应、恢复等五大安全功能，帮助组织建立、评估和持续改善其网络安全风险的闭环应对过程。

5.2.3.3.5 服务组织的系统和组织控制认证 （SOC）

服务组织的系统和组织控制 （SOC） 是由美国注册会计师协会 （AICPA） 创建的内

部控制报告，旨在检查服务组织提供的服务，以便最终用户可以评估和解决与外包服务相关的风险。SOC 1 对与用户实体财务报告的内部控制相关的服务组织中的控制检查进行报告（AICPA 指南）。SOC 2 报告对服务组织中安全性、可用性、处理完整性、机密性或隐私相关的控制进行的检验（AICPA 指南）。SOC 3 适用于服务组织的 SOC：一般用途的信任服务标准报告是面向公众的简短 SOC 2 类型 2 证明报告版本，适用于需要有关安全性、可用性、处理完整性、机密性或隐私相关服务组织控制的保证，但又不需要完整 SOC 2 报告的用户。 由于 SOC 3 报告是一般用途报告，因此可以自由分发。SOC 3 报告包含服务组织管理层关于控制在基于适用信任服务标准实现承诺方面的有效性的书面声明，以及服务审核员对管理层声明是否公平的意见。

5.2.3.3.6 支付行业数字安全认证 PCI DSS

Payment Card Industry Data Security Standard，即第三方支付行业(支付卡行业 PCI DSS)数据安全标准，是由 PCI 安全标准委员会（PCI SSC：Payment Card Industry Security Standards Council）的创始成员（美国运通 American Express、美国发现金融服务公司 Discover Financial Services、JCB、全球万事达卡组织及 Visa 国际组织）共同组建的支付卡产业安全标准委员会制定。是 PCI DSS 一个支持和提高持卡人数据安全和卡组织采用的全球化一致性的数据安全措施，提供了一套保护持卡人数据的技术和操作的基线要求。PCI DSS 信息安全标准有 6 大目标，12 个大类要求，PCI DSS 标准从信息安全管理体系、网络安全、物理安全、数据加密等方方面面提出了诸多的安全基线要求。

5.2.3.3.7 医疗健康数据合规认证 HIPAA

HIPAA 全称为 Health Insurance Portability and Accountability Act/1996，Public Law 104-191，《1996 年健康保险流通与责任法案》。HIPAA 力图推动电子健康记录的采用，以便通过加强信息共享提高美国医疗保健系统的效率和质量。在推动采用电子病历的同时，HIPAA 还加入了相关规定保障受保护健康信息 (PHI) 的安全性和隐私性。PHI 包含一系列非常广泛的可识别个人身份的健康数据和健康相关数据，包括保险和账单信息、诊断数据、临床护理数据、影像等实验室结果以及测试结果。HIPAA 的条例适用于所涉实体，其中包括直接接触病人并处理病人数据的医院、医疗服务提供商、由雇主赞助的健康计划、研究机构和保险公司。HIPAA 还将保护 PHI 这一要求的适用范围扩大到了商业伙伴。

随着《2009 年经济与临床健康信息技术法案 (HITECH)》的颁布，HIPAA 条例得到了进一步的扩充。HIPAA 和 HITECH 共同建立起了一套联邦标准，意在保障 PHI 的安全性和隐私性。这些条款包含在称为“简化管理”的规则中。HIPAA 和 HITECH 强制推行使用和披

露 PHI 的相关要求、保护 PHI 的适当安全措施、个人权利和管理责任。

5.2.3.3.8 汽车信息安全评估和数据交换认证 TISAX

TISAX（Trusted Information Security Assessment Exchange）是德国汽车行业通用的信息安全审核标准，目的是对主机厂和上游客户的敏感信息进行安全的共享和必要的保护，从而提升德国汽车行业整体的信息安全管理水平，全球所有德系汽车相关的供应商（包括零部件厂商、外围服务商等）均应建立和维持信息安全管理体系，并通过与之相应级别的 TISAX 外部审计。

TISAX 使用的标准是 VDA-ISA，该标准是基于 ISO27001/27002，并根据德国汽车行业的特点，增加了原型样车和零部件保护、数据（个人信息）保护的要求，根据不同的信息保护级别（High 和 Very High），以及业务特点的要求，分为两个审核级别 AL2 和 AL3，均需通过第三方外部审核，AL3 还必须现场审核。

目前现行 TISAX®一共定义了 10 个标签。企业通过申请，通过几个，就将获得几个标签。目前标签包括：2 个信息安全标签（INFO HIGH，INFO VERY HIGH）、2 个第三方连接标签（CON HIGH，CON VERY HIGH）、4 个原型保护标签（PROTO PARTS，PROTO VEHICLES）

5.2.3.3.9 其它

日本 Cloud Security Mark (CS Mark) 是日本制定的第一个面向云服务提供商的安全标准。 CS Mark 基于有关云服务的 ISO/IEC 27002，阐述云计算中的信息安全性以及与云相关的信息安全控制措施的实施。CS Mark 由日本信息安全审计协会 (JASA) 认可，该协会一家由内务省和经济产业省建立的非盈利组织，旨在加强日本的信息安全保护。

日本信息系统安全管理和评估计划（ISMAP）是由日本政府管理的云服务评估计划。该计划已于 2020 年 5 月 26 日正式公布，旨在通过评估和注册符合日本政府安全要求的云服务来确保政府云服务采购的安全性。打算参与公共部门采购计划的云服务提供商可以申请由 ISMAP 批准的独立第三方审核公司管理的 ISMAP 认证。 然后，日本政府机构可以从注册到 ISMAP 的云服务提供商处采购云服务，而不是进行自己的独立评估。

韩国信息安全管理系统（K-ISMS）是一个针对特定国家/地区的 ISMS 框架，定义了一套严格的控制要求，旨在帮助确保韩国的组织始终如一、安全地保护其信息资产。要获得认证，公司必须接受独立审计师的评估，评估涵盖信息安全管理和安全对策。涵盖 104 项标准，其中信息安全管理 5 个行业 12 个控制项目，信息安全对策 13 个行业 92 个控制项目。其中一些标准包括检查组织的安全管理职责、安全策略、安全培训、事件响应、风险管理等。K-ISMS 框架建立在成功的信息安全战略和政策之上。它还考虑了安全对策和威胁响应程序，以最大限度地减少安全漏洞的影响。这些程序与 ISO/IEC 27001

控制目标有很大的重叠，但并不完全相同。 K-ISMS 提供了比一般 ISO/IEC 27001 评估更详细的要求。在韩国科学和信息技术部 (MSIT) 的监督下，韩国互联网与安全局 (KISA) 是 K-ISMS 认证机构。认证有效期为三年，认证实体必须通过年度审核才能维持。

新加坡多层云安全 (MTCS) 标准是在新加坡资讯通信发展管理局 (IDA) 信息技术标准委员会 (ITSC) 的指导下拟定的。ITSC 负责推动国家 IT 和通信标准化项目的开展，并协助新加坡参与国际标准化活动。MTCS 旨在提供常用标准，云服务提供商 (CSP) 可采用该标准来解决客户对云端数据的安全性和机密性以及使用云服务对业务的影响的顾虑。可验证的操作透明度，以及对客户在使用云服务时所面临的风险的洞察。MTCS 建立在公认的国际标准（如 ISO/IEC 27001）基础之上，覆盖的领域有数据保存、数据主权、数据可移植性、债务、可用性、业务连续性、灾难恢复和事件管理。该标准还包括一种机制，可供客户按照一系列最低基线安全性要求对各大 CSP 的能力进行标准检查和排名。

BS 10012 是英国标准协会 BSI 发布的个人信息管理体系标准，为个人信息管理体系提供了一个符合欧盟 GDPR 原则的最佳实践框架。它概述了组织在收集、存储、处理、保留或处理与个人相关的个人记录时需要考虑的核心需求。

5.3 数字安全案例

5.3.1 某银行科技子公司隐私和数据安全落地项目

5.3.1.1 案例背景

某银行科技公司为某股份制行的全资子公司，前期已通过多项安全认证体系，但针对数字安全尤其是隐私安全、数据安全、数据治理方面仍有不足，因此需要在隐私和数据安全方面进行体系化提升和平台化的落地，提升数字安全建设水平。

5.3.1.2 案例概述

案例包括隐私和数据安全体系治理和平台化落地两个方面，其中隐私和数据安全体系治理包括云隐私安全、隐私保护和数据治理三个体系，旨在对数据资产全域摸底排查，发现数据安全风险，体系化整体数据保护能力和为平台提供基础支撑数据；平台化一期覆盖金融账单数据这一细分领域，对全生命周期管控和治理进行设计。

5.3.1.3 安全技术方案

数字安全的基础方向之一是构建隐私和数据安全体系治理，根据人机料环法理论，首先完成组织建设，也就是人的方面。

根据数字安全的整体规划要求，在当前组织架构上建立自上而下的数据安全与隐私保护组织架构，落实关键人员角色，对必须岗位拾遗补漏，包括：最高决策者（安全与隐私合规委员会）、安全与隐私保护工作组（牵头某公司隐私工作相关事务）、各业务团队安全与隐私专员（负责本部门或本产品线相关隐私合规与安全要求的上传下达）。其中为了保证数字安全的组织级别落地，由公司首席技术官兼任首席数据安全官，形成总经理办公会级别的安全与隐私合规委员会。

机、料、环三个方面构成平台落地，在这一阶段需要摸排现状，以体系为参考进行调研和评估：梳理业务相关的个人信息数据清单，并基于个人信息处理的生命周期，对个人信息数据流全生命周期的管控现状进行深入调研并予以细化；基于数据安全和隐私保护体系和隐私保护法规要求，同时参考其他个人信息保护标准，识别上述个人信息在其生命周期各个阶段所面临的隐私合规风险和数据安全风险；梳理 DPIA 风险评估结果，分析现状与数据安全和隐私保护体系标准之间的差距，识别个人信息保护现存的高级别风险，开展后续风险处置措施。同时，风险评估与现有风险评估进行有机融合，避免同类型 RA（风险评估）过多导致的资源浪费和损耗。

为遵循合规要求，形成现代化的制度和管理体系。项目内完成隐私合规类内部流程制度，例如：隐私影响评估流程、用户数据主体隐私权响应流程、隐私违规事件处理流程等；完成面向用户数据主体（Data Subject）的隐私协议；完成面向数据控制者（Data Controller）的数据处理协议；完成面向供应商/合作伙伴/生态圈/关联单位（Sub-contractor）的数据处理委托协议等文件。

本阶段工作总结参考下表，为下一阶段数字安全平台的开发奠定了基础。

模块	工作任务分解	工作任务详述	项目产出物

现状调研与差距评估	个人信息管理现状调研与隐私影响评估（DPIA）	1、数据清单（Data Inventory）与数据流（Data Flow）：梳理某公司团队梳理业务相关的个人信息数据清单，并基于个人信息处理的生命周期，对个人信息数据流全生命周期的管控现状进行深入调研并予以细化； 2、数据保护影响评估（DPIA）：基于数据安全和隐私保护体系和隐私保护法规要求，同时参考其他个人信息保护标准，识别上述个人信息在其生命周期各个阶段所面临的隐私合规风险和数据安全风险； 3、风险处置（Risk Treatment）：梳理 DPIA 风险评估结果，分析现状与 数据安全和隐私保护体系 标准之间的差距，识别个人信息保护现存的高级别风险，指导开展后续风险处置措施，包括但不限于：管理流程建立与完善、隐私政策合规性优化、系统平台合规与安全性改进、业务流程合规性改进。	1、业务流个人信息清单（个人信息梳理、个人信息全生命周期现状调研，涉及所有业务环节调研） 2、隐私影响评估（DPIA）过程记录和评估结果（针对上述各业务环节的数据安全与隐私合规风险识别、分析，以及风险分析结果的沟通） 3、隐私影响评估（DPIA）风险处置建议（提出风险处置的建议方案，并就方案进行沟通并达成一致） 4、数据安全和隐私保护体系差距分析结果
数据治理与隐私合规体系建设	数据安全与隐私保护组织架构设计	指导建立其自上而下的数据安全与隐私保护组织架构，落实关键人员角色，包括：最高决策者（安全与隐私合规委员会）；安全与隐私保护工作组（牵头某公司隐私工作相关事务）；各业务团队安全与隐私专员（负责本部门或本产品线相关隐私合规与安全要求的上传下达）。	1、数据安全与隐私保护组织架构图 2、数据安全与隐私保护组织职责清单
	数据治理及隐私合规类文件评审和编写	辅导某公司相关团队梳理、完善某公司隐私合规类文件。包括但不限于： 1、隐私合规类内部流程制度，例如：隐私影响评估流程、用户数据主体隐私权响应流程、隐私违规事件处理流程等； 2、面向用户数据主体（Data Subject）的隐私协议； 3、面向数据控制者（Data Controller）的数据处理协议； 4、面向供应商/合作伙伴/生态圈/关联单位（Sub-contractor）的数据处理委托协议等文件。	1、经过合规性修订的客户隐私协议与合作方数据处理协议。 2、与 ISMS 文件充分整合的流程制度，如： - 隐私数据分类分级规范； - 软件开发隐私默认设计流程； - 隐私影响评估流程； - 用户数据主体隐私权响应流程； - 隐私违规事件处理流程； - 隐私数据披露规范等； -数据治理管理规范等； -云隐私管理规范等，
	数据治理及隐私合规风险技术平台前瞻	根据前期 DPIA 结果，结合隐私合规类内部流程制度建设情况，：针对某公司的业务产品，落实数据治理的管理要求的改进。	为下一阶段的平台落地提供方向性意见。

表 5-1 某银行科技子公司隐私和数据安全项目工作汇总

平台化一直是落地的必经之路和难点，一个能体现数字安全的平台更是难上加难，因此为了保证投资的产出，在第一阶段的产出物中选择适合数字安全的域进行落地，最终选择了多云管理和计费域（MSP），这个域强调金融业务，有大量的账单数据、用户数据和付费数据，对接系统多，对接技术难度大，但业务模式较为单一，个人数据和隐私数据诸多，是数字安全尝试落地的一个好区域。

根据某知名国际组织定义，公共云基础设施 MSP 定义为“为一个或多个超大规模 CIPS 提供商提供与基础设施和平台运营相关的专业和托管服务的提供商。”

MSP 应可采用产品化、模块化、包干化的多种计费模式，具备充值付费和后付费的多种选择，绝大多数产品可以到秒级的计费颗粒。

平台设计要整理清楚商户组织、项目管理（项目户头）、商管账户、产品线（产品线账户）、订单、合同产品线、付费模式的关系。例如在合同签署后，将先提供账单模板给客户付费部门确认，确认后合同期内账单格式将不作调整这样的模式是否可行，需要业务部门的再三确认。

商户管理是一种角色，绑定在某个商管账户下，具有商户管理角色的商管账户可以发起项目邀请（对某个商管账户），一旦接受邀请，该项目下所有商管账户均归属该商户。

项目管理是一种角色，绑定在某个商管账户下，具有项目管理角色的商管账户可以发起对其他商管账户的邀请，其他商管账户一旦接受邀请，受邀商管账户的消费统筹均记在该项目下。一个商管账户只能同时归属一个项目。

项目户头绑定在项目上，是客户充值、余额的最小单位。具有项目角色的商管账户，可以查看本项目下的整体充值、消费、余额和调账情况，以及下属各商管账户的消费情况

项目户头上同时设定信用额度，信用额度代表客户后付费透支的最大限额，超过信用额度的服务质量将难以保障。

商户和项目可以同时挂在一个商管账户下，原则上每个商管账户必须挂在一个项目下，每个项目挂在一个商户下。（如果新创建一个商管账户没有指定好商户或项目，统一挂到“未指定商户”下的“测试项目”中）。

商管账户是云商管登陆的最小单位，商管账户下关联账单和订单，各产品线的订单和账单，只属于一个商管账户。一个客户可能只开通了商管账户，未指定商户和项

目。商管账户是最小服务单位，包含服务经理，客户联系方式等信息。

每个商户账户可以接受邀请加入项目，如果该商户具有项目管理角色，可以接受商户邀请；

每个商管账户对应 0 个或 1 个产品线账户，产品线账户一般只提供计量信息，有的产品线支持产品线账户，且要支持认证跳转，有的产品线可能不支持。

合同需要挂在项目下，合同拆解到不同账户下。

订单有 3 个维度：商管账户、合同、产品线；订单必须归属一个产品线（不能多个），必须挂在一个商管账户下（不能多个），可以挂 0-1 个合同下；

每个订单只能有一种付费模式。客户自助下单或后台录入下单时，需要指定订单的付费方式，原则上一个商管账户的一个产品线的多张订单，只支持同一种付费模式（如产品线自身支持除外）

一个商管账户的账单由该账户下所有的有效订单生成。

基于以上的业务和应用逻辑，再结合安全要求，一期平台建设如下图规划：

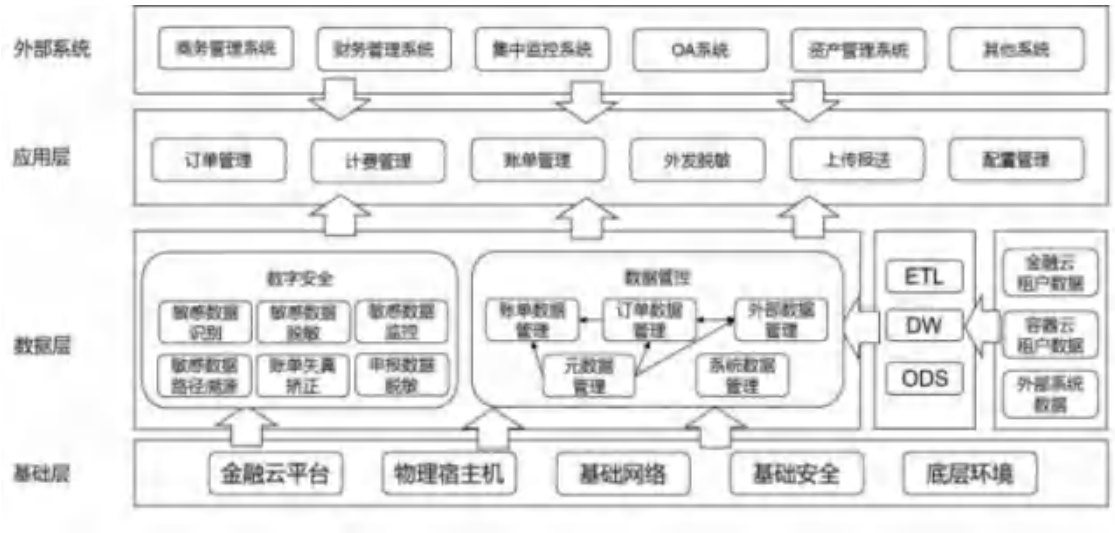


图 5-1 某银行科技子公司隐私和数据安全项目一期平台规划

整体安全考虑包括基础安全、系统安全、数据安全、应用安全和外部对接安全。从而平台分为基础层、数据层、应用层和外部系统接入层。

系统架设在公司金融云 Iaas 侧，金融云底层环境均部署在总行数据中心内，采用 Ti 3+建设标准和知名体系 U&O 进行运维管理。基础安全体系均满足质量控制、运维管理、信息安全等相关体系要求。

金融云 Iaas 具备多副本高可用，资源监控和 AI 报警，宕机自动迁移等多种物理安全措施，还包括云全局的物理安全设施，如态势感知、防火墙、IPS、IDS、HIDS、蜜罐、威胁情报等。

数据层为核心层，数据包括金融云上租户计费数据、容器云租户计费数据和外部系统相关计费数据。其中金融云和容器云上为主数据，外部系统为比对数据。

数据的输入安全采用 ETL、DE、ODS 等多项成熟数据抽取和管理技术进行获取和清洗。元数据包括账单各子模块基准价格，如云主机、网络带宽、防火墙、安全设备、对象存储等，各子模块包含多型号、多品牌数据。元数据还包括计费周期参数列表，基于秒级的计数方式，按流量的计数方式和按次数的计数方式。

数据的存储安全包括账单数据、订单数据、外部数据、三者互相进行验证和比对，元数据和系统配置数据进行整体支撑。

数字安全模块包括数据自身的识别、监控、流转等过程，根据第一阶段的体系成果，对敏感数据进行场景化管理，实现敏感数据的识别、监控、脱敏和溯源。同时针对账单数据，提供了业务等级的失真矫正能力。

数据特征从敏感度、数据时效性、与客户信息关联关系等维度考虑，将数据安全等级分为自小到大多个等级，等级与数据敏感度成正比，等级与生成测试数据的变化程度成反比。

账单失真校准首先依托于多个数据源的校对，如发现常态业务数据量有大幅度波动突破阈值设置，则会进行标记并进行警告通知。失真校准同时具备自动的计费基数比对能力，当发现不适用的计费被错误列入账单同样会进行警告通知。

应用安全围绕业务能力保障和系统自身稳定进行设计，包括订单管理、计费管理、账单管理、外发脱敏、上报报送和配置安全。系统展示界面如下：

图 5-2 某银行科技子公司隐私和数据安全项目一期系统界面

5.3.1.4 案例总结

整个项目最终对某公司的整体数字安全带来提升，为之后的二期项目、数字安全衍生项目和其他信息安全项目奠定了基础，建立的安全组织、数据安全管理体系满足数字安全的要求，满足当前适用的法律法规要求，适合公司业务和环境状况，是充分的、适宜的、有效的。

平台化将项目体系管理部分中的多云管理的账单计费管理进行落地，明确账单计费数据中敏感信息识别、监控、安全预处理、使用、流转等体现数据全生命周期环节的处理流程，根据生产数据中敏感信息数据的相关信息使用符合业务情况的脱敏工具，并明确在生产数据使用过程中所涉及部门的职责分工，提高账单管理使用管理规范化、制度化水平，防范隐私数据泄露等安全隐患，完善风险管理体系。该项目整体获得公司领导层高度认可。

5.3.2 某知名外资汽车金融公司 IAM 管理体系优化项目

5.3.2.1 案例背景

某跨国汽车金融公司是某国际汽车金融服务股份公司的在华全资子公司，总部设立在中国北京，一直致力于为中国的广大汽车消费者提供先进的汽车金融产品和高质量的服务。

该公司与相关汽车集团合作经销商建立了非常积极、紧密的合作关系，一直积极地推广与发展汽车金融业务，通过相关汽车集团经销商网络促进了多款车型进口汽车的在华销售，同时也不断为各类终端消费者提供革新的金融产品和服务。

5.3.2.2 案例概述

随着国内数字经济引擎的爆发力推动，该公司金融业务数字化转型也在大跨步发展，企业内各类数据资产日益庞大且应用环境也日趋复杂。同时，金融管理部门也逐渐加大了转型指导和规范，且更加重视提升企业网络安全保障能力、提高金融数据安全保护要求。

因此，如何在符合国家网络安全法律法规的合规要求，及金融领域内中国人民银行与银保监会的相关监管合规要求的前提下，对企业内各类数据资产的访问和应用进行精细化管理，给数字化经济体系下的企业带来了非常大的挑战。除了数据安全本

身需要采取的分类分级管控外，如何在应用系统层面实现精确的访问控制，需要依靠企业级身份和访问管理（IAM）系统对数据资产的安全访问进行保障。

身份与访问管理安全是数据安全管理的重要基础之一，其目的为全面地建立和维护企业统一数字身份，并提供有效的、安全的 IT 资源访问的业务流程和管理手段。IAM 可以统筹实现企业信息资产访问的统一身份认证、授权和身份数据集中管理与审计，直接掌管着用户及各类电子资产对企业资源、系统和数据的访问权限。

随着数字经济引擎的爆发力推动，企业数字化转型大跨步发展，企业内各类数据资产日益庞大且应用环境也日趋复杂。如何有效地基于安全合规及企业管理的要求，对数据的访问和应用进行精细化管理，就要靠企业级身份和访问管理（IAM）系统对数据安全访问进行保障。

5.3.2.3 安全技术应用方案

IAM（身份和访问管理） 是一个策略、流程和技术框架，使组织能够管理数字身份并控制用户对企业数字资产的访问。通过为用户及各类资产分配特定角色和策略确保其对企业网络和资产具有适当的访问权限。IAM 既可以提高企业数据访问的安全性及各类终端用户的使用体验，同时也能大大提高移动和远程工作以及云资源统一使用与管理的可行性。

运用 IAM 的精细化策略管理，可实现资源的细粒度访问控制，结合企业数据生命周期管理、应用生命周期管理等特性，可以帮助企业打造适合自身的、集数据资产保护与身份和访问管理于一体的 IAM 管理体系。

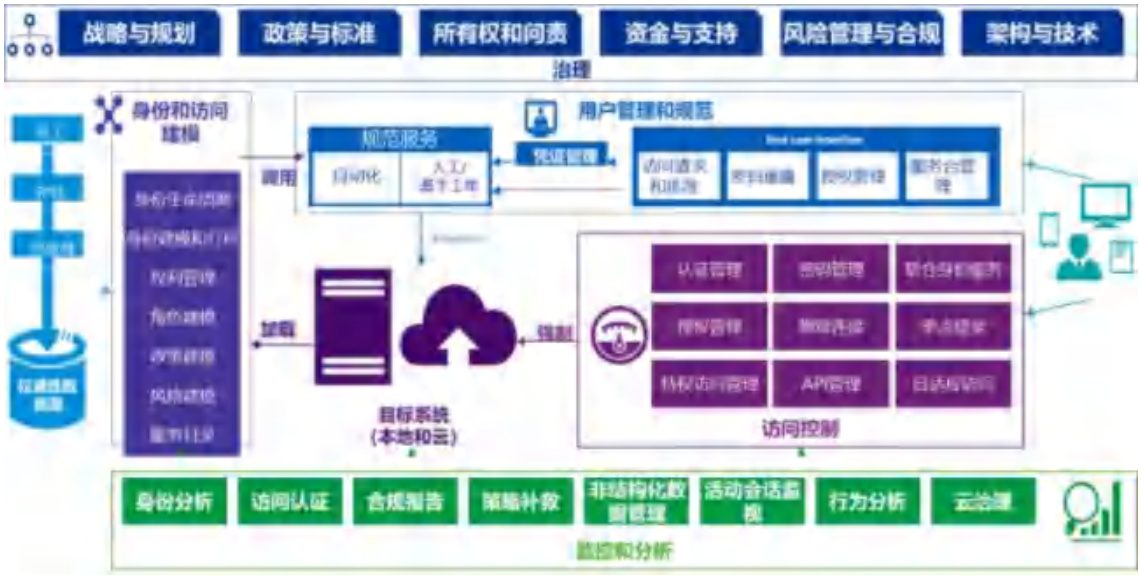


图 5-3 某知名外资汽车金融公司 IAM 管理体系规划

该项目中，基于客户的实际业务环境及安全合规需求，在企业 IAM 管理体系设计的同时，充分将数据安全保护融入其中，从账号管理、认证管理、授权管理及集中审计四个方面对客户的数据和应用资产进行了精细化的访问控制管理。

5.3.2.3.1 账号管理

数据资产的身份和访问管理，需要制定一份基于企业实际的账号管理体系。在账号的设计过程中，基于账号访问资源的不同，对权限级别进行了划分，然后基于不同权限级别的账号结合具体业务流程对账号进行统一体系设计。

- 特殊权限：具有账号的创建、更改、删除；可进行后台操作；非系统个人账号等权限。
- 重要权限：１）可进行金融交易预定授权（如发票、合同等预定）；２）拥有重要业务数据和个人信息访问权限（合同数据、账目查询、征信信息查看等）；３）可以对敏感数据（机密和秘密数据）进行访问和操作的权限。
- 标准权限：可以访问公司相关的公共信息和内部信息的权限。

此外，基于每一个业务应用系统的生命周期管理，基于各应用系统保护等级（基于业务重要性、系统数据重要性等）、架构管理、权限管理、测试管理等不同管理分支，设计对应的授权负责人账号体系，对整体账号体系进行集中管理与监督。

5.3.2.3.2 授权管理

账号的权限一般分为普通允许账号和特权账号。各类账号的权限授予都必须严格执行相应的申请审批流程，尤其是针对特权账号。该项目中，权限的设计主要是基于角色的访问控制（RBAC）模型进行设计；同时，为保障数据资产的合理有效访问，我们结合了基于属性的访问控制（ABAC）模型，在数据分类分级的基础上，针对访问资源中包含数据的属性（敏感程度）对账号权限进行设计。

在账号申请流程方面：

- 没有特殊要求的系统权限可直接在权限管理系统进行申请;对于 RDP、ADM、VPN 等敏感权限，需要走特定的申请流程审批；
- 对每个系统的权限建立权限划分设计 SOD 矩阵，并根据 SOD 矩阵对比审核申请的权限是否符合规范；
- 对核心系统的相关操作人员，禁止申请邮件外发、互联网访问等权限。
- 对于包含敏感数据的应用权限和文件系统，只有特定人员才能进行申请访问，并且只赋予只读权限，防范数据篡改。

另外，对于非账号访问的数据资产间访问（如接口访问、服务调用等）授权，基于访问双方处理数据的级别，对双方对象也做了资产级别划分，基于资产级别和访问调用关系，建立其访问权限设计，并定义不同资产所属者为具体授权方，对相关权限基于流程进行分配或调整。

5.3.2.3.3 认证管理

在身份鉴别方面，基于客户已有的 IAM 系统产品，充分利用多种主流认证集成协议，如 Oauth 协议、SAML 协议、JWT 协议等，对企业内各系统的统一认证接入标准进行定义。同时，基于独立 LDAP 的设计架构建立了自定义开发认证的 API 接口标准。

另外，建立企业级 PKI 及数字证书签发系统，动态口令平台等，在实现各类 PC 端 WEB 应用和移动端应用认证及单点登录集成的同时，提供不同等级安全认证方式，通过用户名/密码、动态口令及数字证书等提高认证安全性，并灵活组合满足应用不同安全级别的双因素/多因素（2FA/MFA）认证要求。

5.3.2.3.4 集中审计

IAM 系统将用户认证、单点登录、自助服务操作、管理员账号操作以及用户状态变化自动产生的日志集中进行收集和存储，根据不同的管理和运维要求基于统一接口提供灵活配置的展示视图。

同时，根据各应用系统的实际业务情况，建立了标准化的审计作业要求。

- 对于 IAM 管理规范中划分的不同权限类型以及系统的保护等级，制定周、月、季度、年度等不同要求的权限审查计划，依据计划定期对权限进行审核，发现异常的权限及时进行确认和删除;
- 对于核心应用，每年对账号 SOD 进行跨系统的审核，比对是否有存在冲突或异常的权限；
- 对于所有有权限管理需求的应用，每年都需要对应用的权限管理文档进行更新，并有权限管理部门进行审核；
- 使用日志管理系统对权限操作进行日志监控，每天对导出的日志内容进行分析，并形成报告，并对异常信息进行确认；
- 积极配合公司的 IT 内审工作，对审计发现的问题进行澄清和整改。

5.3.2.4 案例总结

IAM 管理体系及系统的实施有效解决了该公司内许多数据安全障碍，同时很大程度上改善了组织的安全状况。

该平台改进了公司内各类应用系统和资产的访问活动，加强了公司各类数据资产的访问安全。不但实现了员工、供应商、合作伙伴及消费者对于各类应用系统和数据资产的细粒度访问控制；同时集成 API 安全网关，通过确认 API 的身份、为匹配的 API 授权等，实现各系统软件和软件之间 API 调用访问的认证和权限管理。在确保公司数据安全和满足相应合规要求的同时，为最终消费者提供更加灵活和精细化的系统访问服务。

5.3.3 腾讯 iOA 助力贝壳找房落地零信任安全战略

5.3.3.1 案例背景

贝壳找房是国内房屋中介龙头公司，也是国内最大的住房交易服务平台。贝壳找房由链家网升级而来，是以技术驱动的品质居住服务平台，致力于为三亿家庭提供包括二 手房、新房、租赁、装修和社区服务等全方位居住服务。 经过 20 年的发展，截止 2020 年末，链家已经拥有 13.9 万名经纪人、7800 家门店。通过贝壳构建的经纪人合作网络（ACN），贝壳重建了整个行业内各参与者的关系。 通过 ACN 模式，贝壳可以促进经纪品牌、门店、代理商的合作，简化交易流程。同 时，贝壳还为平台参与者提供各种数字化服务，包括 SaaS 系统、客户前端、以社区 为中心的商店网络、数据洞察和技术应用、金融服务、培训和招聘计划以及交易服务 中心等。

5.3.3.2 案例概述

随着贝壳找房业务地快速扩张，员工和门店的终端管理始终面临巨大的挑战。贝壳找 房的企业信息安全管理除了需要面对监管合规要求、传统的安全威胁之外，还要面临 自身产业特点所带来的挑战。贝壳找房在业务管理上的数字化程度本身就比较高，但在长期的运维过程中，IT 管理部门无法有效的应对以下挑战：

- 贝壳找房的网络接入点数量大且情况复杂。贝壳拥有数千家门店、职场，以及数 十万经纪人员工，这些员工的终端采用不同的网络接入方式、业务访问情况复杂，安 全无统一管理，消耗大量管理资源且效果不佳。
- 贝壳找房的对外合作多。贝壳在整个居住领域要扩展新的赛道、要链接更多的服 务，对内部服务的对外开放灵活性也有了更多效率上的期待。
- 贝壳找房的业务处理过程高度依赖核心敏感数据。经纪人作业过程中、对外交互时涉及很多核心敏感数据，数据可能散落在各个网络接入点中，数据的边界是相对模糊的。

5.3.3.3 安全技术方案

贝壳找房通过部署腾讯的 iOA 零信任管理系统，实现以下关键的零信任管理能力：

- 腾讯 iOA 零信任安全管理系统集成安全防护、补丁管理、安全管控、零信任接入、 数据安全、网络准入等终端办公安全相关的能力，为贝壳找房提供办公环境 终端统一安全管理解决方案。在提升终端安全管理能力的同时，降低管理和部署成本， 并为终端用户提供更好的使用体验。
- 腾讯 iOA 零信任安全管理系统能够与贝壳找房已有的身份管理系统（IAM）进行标准化对接，基于用户的不同角色提供业务访问权限的精细化管理。同时，通过动态 策略评估功能，实现可信身份、可信设备、可信应用和可信链路的“4T”安全访问。
- 腾讯 iOA 零信任管理系统通过异地双云的集群化部署，为贝壳找房构建了可无缝扩容，并提供容灾保护的部署方式。在确保高并发、高性能业务访问的同时，提升了 用户的访问体验。

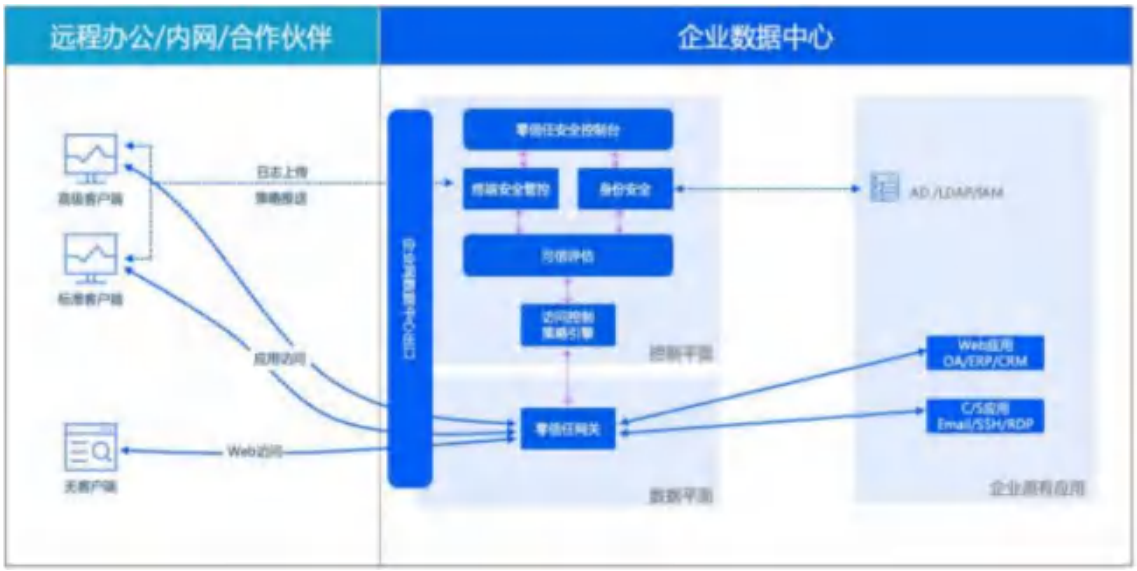


图 5-4 贝壳找房落地零信任系统架构示例

贝壳找房通过部署腾讯安全的 iOA 零信任安全管理系统，实现全集团超过 40 万终端 的统一安全管理和零信任接入。依托腾讯在零信任落地上的最佳实践，帮助贝壳落地办公安全方面的零信任安全战略。在提升安全管理效率的同时，降低了在终端安全 管理上的成本，为贝壳找房业务的发展提供了坚实的安全保障。

- 腾讯 iOA 通过终端一体化方案将原有杀毒、管控、VPN、准入、DLP 等需要单独部署的安全管理能力通过单个客户端完成。在减少系统资源占用的

同事，提供最佳的安全防护效果。

- 零信任作为当前 VPN 的最佳替代方案也成为贝壳远程业务安全接入的最佳选择，既避免了 VPN 频发漏洞带来的风险，又以软件化弹性部署实现的门店无缝覆盖。
- 腾讯 iOA 提供的统一业务办公门户，在降低员工登录门槛的同时，无缝对接 IAM 实现业务访问单点登录，有效提升了员工的工作效率和办公体验。
- 腾讯 iOA 的 DLP 模块通过与贝壳找房的业务场景结合，实现业务数据全流程透明 审计，有效提升了业务数据的安全性。

5.3.3.4 案例总结

依托腾讯安全成熟的交付实施服务，整个集团在 3 个月内顺利完成了几十万终端的推 广工作。腾讯的 iOA 产品不仅提升了 IT 部门对全网终端的安全管理能力，也降低了 在终端安全管理上的运维成本。在降低企业 IT 安全风险的同时，为业务快速扩张保驾 护航。通过部署腾讯的 iOA 零信任解决方案，有效降低了贝壳的系统性安全风险，为 贝壳内部零信任战略的落地打下了坚实的基础。

5.3.4 某知名国际电子支付公司数据加密体系构建项目

5.3.4.1 案例背景

某国际知名电子支付公司是一家全球性的支付技术公司，致力于帮助消费者、企业、银行和政府使用数字化货币。该公司通过提供支付产品平台和支付清算服务，连接全球各地的金融机构、商户和持卡人，实现更快速、更便捷、更可靠、更安全的支付网络。同时，该公司不断研究如何利用其规模化的网络资源和先进的支付技术，使世界各地更多的人以更多的方式享受到电子支付带来的价值。由于市场的全球拓展，尤其是对中国市场的开发，其对数据加保护有更多需求，需要符合中国规范化要求的数据安全解决方案提供商，为符合中国市场业务、同时与其国际业务融合提供数据保护的产品方案和服务。

5.3.4.2 案例概述

该公司的核心网络是世界最大的交易和信息处理网络之一，其业务系统一直将安全性作为首要的目标。随着全球业务的扩张，以及在中国境内的业务落地，需要跨各数据处理中心的完善的数据保护解决方案，实现包括业务程序，数据库，文件系统以及大数据系统的安全防护，以此保护其数据资产的机密性和完整性，同时为客户信息的隐私性提供技术支撑。此外，由于政策原因，新扩展的区域如中国区域需要

满足当地特定的合规要求。

密码技术是数字安全的基础技术，在整个安全体系中，数据的机密性、完整性，身份的真实性，交易的不可否认性都是通过密码技术来解决的。随着数字经济的发展，密码技术也越来越多的与各种业务场景深入融合，在各个领域发挥着越来越重要的作用。

该项目将客户需求与密码技术深度结合，实现敏感数据的加密和保护。项目的建设目标包括：

- 保护由业务用例驱动的数据，并跨多个数据保护功能层（应用层、DB 层、文件层）和异构平台（虚拟机、Linux、Windows、AIX、Oracle、DB2、MSSQL、Linux、zTPF、zOS、zVM），以及跨数据保护的全生命周期（DAR、DIT、DIU），实现各种数据分类的一致性保护（PAI、PII、非结构化数据和结构化数据）。
- 实现基于密钥管理的集中策略管理，与企业 IAM、日志、监视和警报集成，实现数据的监视、管理和控制能力。支持跨应用程序边界的安全数据交换，以最少的努力执行良好和一致的密码实践。
- 降低加密和密钥管理的复杂性，使面向全球的开发、集成和发布更加简单。

企业的数据保护现状不容乐观，单就数据加密一项技术来说，该项目所面临的挑战就有很多：

- 要面临多供应商平台和多数据层面的异构 IT 环境。一般各类数据保护方案都只能适用于特定的 IT 架构，从企业角度规划的全面的数据保护方案的实施，需要跨应用程序、数据库、文件系统、大数据系统等多数据层面的解决方案能力。
- 要实现数据保护体系的整体性。基于密码学的数据保护体系在理论上是完备的，但在工程实现上存在着诸多问题，密钥管理的碎片化导致与密钥配合的策略无法统一，系统内充斥着大量的密钥或敏感秘密信息明文流转和存储，新的 IT 项目增加的数据点无法快速纳入之前的保护体系。因此除异构问题之外，对数据全生命期的加密体系构建也是一个难题。
- 合规问题。企业面临内部和外部的合规需求，面向内部的知识产权保护，以及构建数据安全港来施行企业的数据使用规范，防止内部或外部的数据滥用是主要需求。面向外部，跨国企业在新的区域扩张所面临的当地法律政策要求也是必须要重视和规避的。密码技术一直以来是构建国家数字边界的核心技术，因此必须要求其供应商有对各区域合规政策的深入了解，

并将其加入到自己产品的能力中。

5.3.4.3 安全技术方案

本方案以 SecKMS 密钥管理产品为核心，构建了一整套数据保护解决方案。

图 5-5 某知名国际电子支付公司数据加密体系方案示例

SecKMS 提供基于 KMIP 的密钥全生命周期管理以及远程加密服务，SecDB、SecBD、SecApp、Secstorage 等各组件利用 KMIP 管理自己的密钥，并相应对数据库，业务程序，大数据系统和文件系统提供数据加密保护。SecKMS 使用自主研发的 HSM 硬件储存和保护系统密钥。

密钥管理部分根据国际标准定义密钥生命周期，对密钥体系中各类密钥提供全生命周期的管理，对 DEK 提供轮换功能，并提供密钥版本号维护功能。

方案的权限管理与公司级 IAM 融合，将密钥管理与数据的访问权限管理深度绑定，所有方案的组件、插件及 API 都作为数据的访问控制点，在使用时进行权限检查，然后才对数据进行加解密处理。这样通过加密能力的全面实施，客户可以实现通过密钥管理，对数据划分逻辑上的安全分域，并对数据的访问角色进行更细粒度的控制。权限的设置通过如下各层做到了充分的细粒度和灵活组合。

图 5-6 某知名国际电子支付公司数据加密体系密钥管理

请求密钥的身份：客户端 API 请求密钥时，需提交其身份证明，可支持应用名或数字证书的方式验证客户端身份。应用被注册到某个用户命名空间下，仅当密钥属于该应用时，应用才有权限访问密钥；

- 访问密钥的凭据：凭据（Secret）是一组秘密信息，用于对密钥访问进行权限验证，管理员可管理凭据的有效期
- Token：为避免每次密钥请求都重新验证凭据，KMS 可配置为返回一个 Token，在 token 的有效期内，应用可以直接通过 Token 表明身份，获取密钥，简化密钥获取过程。
- 密钥所处生命周期状态：密钥拥有状态包括预激活，激活，注销，销毁，彻底删除以及泄露等状态。KMS 会根据当时的密钥状态决定是否允许密钥被获取。

为了更好的支持异构 IT 设施，产品中引入了对国际密钥管理互操作协议 KMIP 的支持，并且作为牵头单位将该协议引入国标。对于那些拥有多个加密工具的大型企业，KMIP 主要解决了需要使用密钥的加密系统与生成和管理这些密钥的密钥管理系统之间的通信标准化问题。通过这些互操作性，不管是企业选择哪款产品或者哪家厂商，企业部署一个密钥管理架构就可以管理企业中的所有加密系统。

方案所支持三方系统包括：

支持的三方系统	数据库	Mysql、MariaDB、Oracle、SQLServer、DB2、MogonDB、PostgreSQL、达梦
	大数据	Hadoop、FI HDFS、Hortonworks、CDH、华三大数据
	存储	windows&Linux 文件系统、windows&Linux 磁盘、NAS、GPFS、OPEN ECM、HUAWEI Oceanstor
	虚拟服务器	Vsphere、Openstack
	云服务	S3、Swift
	Web 中间件	Weblogic、WebSphere、Tomcat、Jboss
	其他	KafKa

表 5-2 某知名国际电子支付公司数据加密体系所支持三方系统

API 接口是 KMS 业务的主要承载方式，也是可独立运行的密码算法 SDK 包，为此我们增加了三种主要特性：

- 客户端 KeyCache：安全获取密钥的 wrap 或数字信封，根据密钥策略缓存密钥，在缓存阶段保护密钥的存储安全；
- 本地加密算法库：在 Application 端独立运算的加密库，使用 KeyCache 的密钥缓存，不需要依赖服务端，可在离线环境中使用
- 服务端加密算法库：调用服务端加密运算服务，返回运算结果，不需要依赖客户端密钥缓存，提高密钥安全性，需要联网环境；

为更好的和应用集成，方案提供了丰富的接口类型和算法支持：

- 密钥操作功能：密钥生成、激活、分发、更新\轮换、导入\导出、注销、销毁、归档、备份\恢复
- 密码运算功能：加密\解密、签名\验签、Mac、Hash
- 开发接口类型：RESTFUL API、Java、C/C++、.NET、SOAP、GO、CAPI
- 接口协议：国密 GM/T0018 接口、KMIP、OpenSSL、JCE、PKCS#1、PKCS#5、PKCS#7、PKCS#8、PKCS#11、PKCS#12、TLS/SSL1.3
- 加密算法类型：对称算法：SM4，AES。非对称算法：SM2，RSA，ECC。HASH 算法：SM3，SHA-1，SHA-2。MAC 算法：HMAC_SM3， HMAC_SHA2

在合规性方面，SecKMS 已通过国家密码管理局的产品认证，整套方案也参照国家相关等保、密评及密码行业标准构建，同时为满足 PCI-DSS 要求，项目中所使用的密码机 SecHSM 通过了 FIPS140-2 Level3 级产品认证，这也是中国第一个得到 FIPS 认证的 HSM 产品。

5.3.4.4 案例总结

该项目历时 2 年多，通过各种实施的平滑过渡，顺利完成了基础能力的测试和上线。整套数据保护方案从三个方面大大提升了公司 IT 基础设施层面的数据安全性。首先，基于密钥的精细管理，实现了对数据的全生命周期的防护，极大降低了外部攻击或系统运维过程中的数据泄露风险；其次，为规避合规风险，方案基于 PCI-DSS 标准，满足公司内部 PAI/PII 数据的保护需求，为在全球范围内匹配个人信息相关法律提供了基础技术平台；同时，面向跨全球区域的场景提供完善的高可用和高一致性解决方案，使数据保护能力匹配支付业务的低延迟和实时可用的基本要求，为后期更大范围的应用打下坚实基础。

该方案综合了跨多中心、多环境的运行方案，在金融级高可用方面积累了经验，构建了一套与国外同类厂商比肩的密码能力架构，也构建了一套密码技术栈，随着应用场景的不断丰富，该技术栈也将更加完备充实。

第六章 总结与展望

近年来，数字经济正在成为一股关键力量，在重组全球要素资源、重塑全球经济结构、改变全球竞争格局中起到关键作用。全球正处于新一轮科技革命和产业变革之中。数字技术正全面向经济社会各领域渗透，其中以大数据、互联网、人工智能、物联网为代表。目前全球已进入数字经济时代：从万物互联、数据驱动、软件定义、平台支撑、智能主导等主要特征中便可得到验证。“加快数字化发展，打造数字经济新优势，协同推进数字产业化和产业数字化转型，加快数字社会建设步伐，提高数字政府建设水平，营造良好数字生态”……这些诉求，无一不折射出数字化的发展大势。

6.1 数字时代

1998 年美国商务部发布了一份题为《浮现中的数字经济》的报告，提出了这样的观点：对经济起决定作用的核心资源，将由“货币”变为“信息”。随着互联网、大数据、云计算、人工智能、区块链等新一代信息技术快速发展，数字化正成为重组全球要素资源、重塑全球经济格局、改变全球竞争格局的重要手段。人类已经处于数字时代的潮流中，数字经济、数字政府、数字军事、数字社会、数字文明等都在加速推进中。近年来比较火热的虚拟世界、元宇宙也是数字时代的产物。数字经济作为一种新的经济形态，比重正在逐年增加；数字政府让民众可以随时随地利用任何设备获取政府信息和服务；数字社会让整个社会的运转基于数字；元宇宙更是建立了一个新的数字世界。

二十年来，数字经济获得了高速发展。以 2020 年的数据为例：

规模上，发达国家数字经济规模达到 24.4 万亿美元，占全球总量的 74.7%，是发展中国家的约 3 倍；

占比上，发达国家数字经济占 GDP 比重为 54.3%，远超发展中国家 27.6%的水平；

增速上，发展中国家数字经济同比名义增长 3.1%，仅略高于发达国家数字经济 3.0%的增速。

数字时代的特点是技术提高了经济和社会中知识周转的速度和广度。数字时代可以看作是一个进化系统的发展，在这个系统中，知识的周转率不仅非常高，而且越来越不受人类的控制，使我们的生活变得更加难以管理。

6.2 数字安全

随着全球数字化进程的蓬勃发展，技术和数据深度融合的数字化经济模式为许多行业带

来了全新的思路与挑战。消费者的数据安全和用户的隐私保护工作从线下转至了线上，海量数据也催生出了许多数据安全管理问题。伴随数字化技术更广泛和深入服务于社会经济，其安全问题带来的后果将更为严峻。面对不断加剧的安全风险，单兵作战已经无法应对，保障数字安全需要打破各自为战局面，实现协同联防。数字安全不是一个单纯的技术问题，是涉及业务、管理、流程、团队等各方面的系统工程。数字经济的高质量发展涉及政策、法律、技术等多领域的协同，需要构建具备原生一体的安全能力，以数字安全可信为本，才能为数字时代保驾护航。

世界各国都在持续优化数据安全政策环境。欧盟发布的《欧洲数据保护监管局战略计划（2020-2024）》，从前瞻性、行动性和协调性三个方面继续加强数据安全保护，保障个人隐私权。美国发布《联邦数据战略与 2020 年行动计划》，确立了保护数据完整性、确保流通数据真实性、数据存储安全性等基本原则。

强化数据及个人信息保护方面的立法也纷纷出台。阿联酋和新西兰分别出台《数据保护法》和《2020 年隐私法》，加强了对数据安全及个人隐私保护的规制建设。日本和新加坡完成了对本国《个人信息（数据）保护法》的修订，明确了个人数据权利及外部使用限制。加拿大出台的《数字宪章实施法案 2020》，提出了保护私营部门个人信息的现代化框架。《中华人民共和国数据安全法》于 2021 年 6 月 10 日公布并于 2021 年 9 月 1 日施行，同年《中华人民共和国个人信息保护法》于 8 月 20 日通过并于 2021 年 11 月 1 日施行。中国随着数据领域和国家安全领域的重要法律出台，数据安全监管思路更为清晰和全面。

欧盟发布《为保持欧盟个人数据保护级别而采用的数据跨境转移工具补充措施》为数据跨境流动中的数据保护问题提供了进一步指导。西班牙数据保护局发布《默认数据保护指南》，阐释了默认数据保护原则的策略、实施措施、记录和审计要求等内容，为企业实践数据保护原则提供具体指导。中国《数据出境安全评估办法》于 2022 年 5 月通过，并于 2022 年 9 月 1 日起施行，规定了数据出境安全评估的范围、条件和程序，为数据出境安全评估工作提供了具体指引。

数字安全以数字身份为核心，以原生安全为基础底座，涵盖了信息安全、网络安全、数据安全、隐私保护等领域或场景，并可扩展以满足数字经济和技术的发展。除此之外，数字安全还包括利用数字技术保障数字基础设施的物理安全。新一代的数据安全遵循“原生安全 Native Security”的核心理念，秉承“天然一体、主动免疫、始终验证、持续防护”的原则，具有“原生一体、安全可信”，覆盖“动静用转”和“云网边端”，真正实现数字可信与安全。

《CSA 2022 数字安全报告》基于 CSA 提出的数字安全 REE（监管、执行和评估）框架，根据数字安全定义定义分为不同域，涵盖了领先的框架、流行的技术以及公认的认证及服务提供商，还包括全球范围内的重要法律，目的在于简要介绍数字安全的全景。《CSA 2022 数字安全报告》可以成为数字安全的参考资料，帮助人们构建更安全的数字环境。

6.3 数字时代的新一代数据安全

数字时代涵盖数字经济、数字政府、数字社会、数字商业、数字生活和数字个人等场景，其建设需要以云计算、大数据、AI、物联网、区块链、5G 等为代表的数字技术的支撑，数据作为数字经济关键要素，实施数据战略、积累数据资源、保障数据安全、做大做强数据产业，已经成为世界各国共同的战略选择。在 2022 年 6 月审议通过的《关于构建数据基础制度更好发挥数据要素作用的意见》中强调，从数据产权、流通交易、收益分配、安全治理等方面，加快构建数据基础制度体系。数字经济的高质量发展需要数字技术构成的基础设施具备原生一体的安全能力，以数字安全可信为本，为数字时代保驾护航。

早期的数据安全--“静态”安全：

早期的数据安全还是被囊括在信息安全的大范畴以内，主要聚焦于数据静态存储的安全管理，以加解密技术为主要研究方向，将数据的安全管理范围局限在有权限接触到数据的用户，以相对闭塞的静态管理模式来保护数据安全，所以其关键是加密算法和密钥的管理，包括生成、使用、发布、销毁、替换等，但随着时代的迅猛发展已无法应对激增的业务需求与复杂的技术迭代，同时也难以应对动态威胁、管控传输和使用过程中的新型风险类型。

当前传统的数据安全--“动静用”安全：

当前传统的数据安全已经提升到了网络安全的范畴，是在早期的数据静态存储安全的基础之上，针对数据的存储（静）、传输（动）和使用（用）过程中的风险与威胁，提供各种安全机制；传统的数据安全对数据的整个生命周期管理提出了更为全面的要求，包括云网边端和“动静用”，从硬件、OS、到应用、中间件和业务及运维，以“事前防范、事中阻断、事后追溯”为防护原则，力求在最大程度上提高数据的安全性。但传统的数据安全仍然存在一定的缺陷，比如其外挂堆砌式被动防堵机制，不具有天然主动免疫的功能，依旧在面对当下多样动态威胁与攻击时略显疲态。

新一代数据安全--“原生一体、安全可信”和“动静用转”：

遵循“原生安全”的核心理念，秉承“天然一体、主动免疫、始终验证、持续防护”的原则，新一代数据安全具有“原生一体、安全可信”的优异特性，覆盖了数据生命周期中的“动静用转”，同时也涵盖了硬件层面的“云网边端”，真正实现数字可信与安全。值得一提的是，在面对数据流动的全球化、地域属性的合法合规监管等复杂外部环境变化时，新一代数据安全能够及时监管到数据在使用、交易、分享及流转等过程中的权利、权益及权限的变化，能够对数据的生产者、拥有者、存储者、传输者、处理者、使用者、计算方、调度方、管控者和监管者动态划拨角色权限，充分保障了跨行业、跨职能、跨地域、跨组织等各方权益，为打破数据孤岛、实现共享共赢筑牢合规可监管基座，支持多次交易，有效防范供应链、合作伙伴、外贼、离在职人员、流氓勒索等各种风险威胁，激发各大数据平台和交易所内动力，做到数据可信与安全。

新技术带来新挑战，新挑战需要新思维，新思维创造新机会。数据作为至关重要的生产要素，需充分发挥数据作为生产要素的重要价值和意义，数据安全必须放在首要位置，新一代数据安全的落地亟需数据安全法律、治理、技术多维并举。

法律与治理层面

在法律与治理层面，数据生产要素要充分发挥作用，不仅需要解决数据权属、确权、定价问题，更需要解决数据权利、权限和权益的分离及流转交易保护问题，使得数字资产不再成为孤岛，可以被多次交易和流转，并且受到权益相关人的管控。

技术层面

在技术层面，要使数据始终处于控密双态计算（Control & Crypto Computing），实现“动静用转”和“云网边端”全面覆盖。确保环境、模型、算法、算力和用户身份的安全可信，进而保障数据在使用和流转中的安全可信。以应对使用、流转、分享、交易状态下的威胁与挑战，防范权利、权益和权限的变化所带来的风险，保障数据的生产者、拥有者、存储者、传输者、处理者、使用者、计算方、调度方、管控者和监管者等各方的利益，保障使用时的安全。

控态包括传控（控态传输）、存控（控态存储）、用控（控态使用）和转控（控态流转）等，保障数据全环节全生命周期的管控，数据与安全可信原生一体，不仅安全而且可信，包括用户、通讯、环境、代码、计算、数据、展现、监管等的安全可信，涉及零信任、云原生、访问管控、隐私计算、可信计算、区块链、分布计算/存储等技术。数据被保护对象与防护机制“孪生同体”、“密不可分”，在存储计算通讯的同时并行进行实时安全可信防护，逐级验证构建可信链条，提供存储计算通讯的安全可信，确保数据资源和操作全程可测可控，提供安全可信的存储计算通讯环境“主动免疫”。

密态包括密传（密态传输）、密存（密态存储）、密用（密态使用）和密转（密态流转）等，保护数据的私密性，涉及加密、混淆、差分、脱敏、ZKP、TEE、隐私计算等技术。同时，数据与其相关方的权利、权限和权益与数据同体共生，支持数据确权、定价、使用、流转和处理，实现数据在“动静用转”的密不透风。

控密双态互补相成，根据数据分级分类、敏感度、合规要求、及成本，双态能够同时存在也可单一存在，遵循“原生安全 Native Security”的核心理念，秉承“天然一体、主动免疫、始终验证、持续防护”的原则，覆盖数据“动静用转”和“云网边端”场景与环境，真正实现新一代数据安全的目标，充分发挥数据的巨大价值，保护数据和隐私，保障数据相关各方的利益，并做到合规可监管，极大帮助数据安全治理，确保数据的充分利用，为数字时代保驾护航。

CSA GCR cloud security alliance GREATER CHINA REGION

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网:https://c-csa.cn 电话:0755-86548359
地址:上海市浦东新区东育路255弄5号3FB30(前滩国际经济组织集聚区)/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905