中国国际金融股份有限公司
关于亚信安全科技股份有限公司
2024 年度持续督导跟踪报告

中国国际金融股份有限公司（以下简称“中金公司”或“保荐机构”）根据《证券发行上市保荐业务管理办法》《上海证券交易所科创板股票上市规则》和《上海证券交易所上市公司自律监管指引第11号——持续督导》等相关规定对亚信安全进行上市后的持续督导工作，并出具本持续督导年度跟踪报告。

一、保荐机构持续督导工作情况

序号	工作内容	持续督导情况
1	建立健全并有效执行持续督导工作制度，并针对具体的持续督导工作制定相应的工作计划	保荐机构已建立健全并有效执行持续督导工作制度，并针对具体的持续督导工作制定相应的工作计划
2	根据中国证监会相关规定，在持续督导工作开始前，与上市公司或相关当事人签署持续督导协议，明确双方在持续督导期间的权利义务，并报上海证券交易所备案	保荐机构已与上市公司签署了《保荐协议》，协议明确了双方在持续督导期间的权利和义务，并已报上海证券交易所备案
3	持续督导期间，按照有关规定对上市公司违法违规事项公开发表声明的，应于披露前向上海证券交易所报告，并经上海证券交易所审核后在指定媒体上公告	2024年度，上市公司未出现按有关规定须保荐机构公开发表声明的违法违规情况
4	持续督导期间，按照有关规定对上市公司违法违规事项公开发表声明的，应于披露前向上海证券交易所报告，并经上海证券交易所审核后在指定媒体上公告	2024年度，上市公司未出现按有关规定须保荐机构公开发表声明的违法违规情况
5	持续督导期间，上市公司或相关当事人出现违法违规、违背承诺等事项的，应自发现或应当发现之日起五个工作日内向上海证券交易所报告，报告内容包括上市公司或相关当事人出现违法违规、违背承诺等事项的具体情况，保荐人采取的督导措施等	2024年度，上市公司及其相关当事人未出现违法违规或违背承诺等事项
6	督导上市公司及其董事、监事、高级管理人员遵守法律、法规、部门规章和上海证券交易所发布的业务规则及其他规范性文件，并切实履行其所做的各项承诺	保荐机构督导上市公司及其董事、监事、高级管理人员遵守法律、法规、部门规章和上海证券交易所发布的业务规则及其他规范性文件，切实履行其所做出的各项承诺
7	督导上市公司建立健全并有效执行公司治理制度，包括但不限于股东大会、董事会、监事会议事规则以及董事、监事和高级管理人员的行为规范等	保荐机构督促上市公司依照相关规定健全完善公司治理制度，并严格执行公司治理制度

序号	工作内容	持续督导情况
8	督导上市公司建立健全并有效执行内控制度，包括但不限于财务管理制度、会计核算制度和内部审计制度，以及募集资金使用、关联交易、对外担保、对外投资、衍生品交易、对子公司的控制等重大经营决策的程序与规则等	公司在2023年2月25日至2023年4月6日期间存在使用闲置募集资金进行现金管理超出董事会授权期限的情形。因前述事件，江苏证监局对公司、时任财务总监出具警示函措施。公司已于2024年11月15日召开董事会、监事会、独立董事专门会议对相关空窗期审议追认。除此之外，保荐机构对上市公司内控制度的设计、实施和有效性进行了核查，上市公司的内控制度符合相关法规要求并得到了有效执行，能够保证公司的规范运行
9	督导上市公司建立健全并有效执行信息披露制度，审阅信息披露文件及其他相关文件，并有充分理由确信上市公司向上海证券交易所提交的文件不存在虚假记载、误导性陈述或重大遗漏	保荐机构督促上市公司严格执行信息披露制度，审阅信息披露文件及其他相关文件
10	对上市公司的信息披露文件及向中国证监会、上海证券交易所提交的其他文件进行事前审阅，对存在问题的信息披露文件及时督促公司予以更正或补充，公司不予更正或补充的，应及时向上海证券交易所报告；对上市公司的信息披露文件未进行事前审阅的，应在上市公司履行信息披露义务后五个交易日内，完成对有关文件的审阅工作，对存在问题的信息披露文件应及时督促上市公司更正或补充，上市公司不予更正或补充的，应及时向上海证券交易所报告	2024年度，公司归属于上市公司股东的净利润为959.06万元，扣除非经常性损益后归属于上市公司股东的净利润为-1,625.66万元，保荐机构认为该事项属于应当进行专项现场检查的情形。2024年4月28日保荐机构对公司进行了现场检查，通过高管访谈、查阅相关公告文件和财务资料等方式对公司经营情况、财务情况以及未来发展进行了研究，了解公司2024年度公司扣除非经常性损益后归属于上市公司股东净利润为负的主要原因
11	关注上市公司或其控股股东、实际控制人、董事、监事、高级管理人员受到中国证监会行政处罚、上海证券交易所纪律处分或者被上海证券交易所出具监管关注函的情况，并督促其完善内部控制制度，采取措施予以纠正	2024年度，上市公司及其相关当事人未出现该等事项
12	持续关注上市公司及控股股东、实际控制人等履行承诺的情况，上市公司及控股股东、实际控制人等未履行承诺事项的，及时向上海证券交易所报告	2024年度，上市公司及其相关当事人不存在未履行承诺的情况
13	关注公共传媒关于上市公司的报道，及时针对市场传闻进行核查。经核查后发现上市公司存在应披露未披露的重大事项或披露的信息与事实不符的，及时督促上市公司如实披露或予以澄清；上市公司不予披露或澄清的，应及时向上海证券交易所报告	2024年度，上市公司未出现该等事项
14	发现以下情形之一的，督促上市公司做出说明并限期改正，同时向上海证券交易所报告：（一）涉嫌违反《上市规则》等相关业务规则；（二）证券服务机构及其签名人员出具的专业意见可	2024年度，上市公司及相关主体未出现该等事项

序号	工作内容	持续督导情况
	能存在虚假记载、误导性陈述或重大遗漏等违法违规情形或其他不当情形；（三）公司出现《保荐办法》第七十条规定的情形；（四）公司不配合持续督导工作；（五）上海证券交易所或保荐人认为需要报告的其他情形	
15	制定对上市公司的现场检查工作计划，明确现场检查工作要求，确保现场检查工作质量	2024年度，保荐机构制定对上市公司的现场检查工作计划，明确现场检查工作要求，确保现场检查工作质量
16	上市公司出现下列情形之一的，保荐机构、保荐代表人应当自知道或者应当知道之日起十五日内进行专项现场核查：（一）存在重大财务造假嫌疑；（二）控股股东、实际控制人、董事、监事或者高级管理人员涉嫌侵占上市公司利益；（三）可能存在重大违规担保；（四）资金往来或者现金流存在重大异常；（五）上海证券交易所或者保荐机构认为应当进行现场核查的其他事项	2024年度，上市公司及相关主体未出现该等事项

二、保荐机构和保荐代表人发现的问题及整改情况

无。

三、重大风险事项

公司目前面临的风险因素主要如下：

（一）核心竞争力风险

1、技术不能保持先进性的风险及相关技术迭代风险

自公司成立以来，公司始终将研发创新放在重要地位，经过多年的研发投入和技术沉淀，公司已掌握多项核心技术，为产品竞争力提供了坚实的支撑。但伴随着计算机、互联网和通信技术的高速发展，科技水平不断进步与创新，各种威胁信息系统安全的手段也层出不穷，信息安全漏洞危害性越来越大，这对公司的技术水平和研发能力提出了较大的挑战。另一方面，尽管公司一直致力于科技创新，力争保持在数智化、网络安全领域的技术领先优势，但不排除国内外竞争对手或潜在竞争对手率先在相关领域取得重大突破，而推出更先进、更具竞争力的技术和产品，或出现其他替代产品和技术，从而使本公司的产品和技术失去领先优势。

2、新产品的研发风险

公司的业务收入由网络安全业务和数智业务两大板块构成，两大业务领域已在众多行业领域取得良好的发展，未来公司将在现有业务的基础上，持续拓展新的业务领域。软件与信息技术服务业的发展日新月异，行业发展趋势存在不确定性，可能会导致公司在新技术的研发方向、重要产品的方案制定等方面不能及时做出准确决策。公司可能面临新产品研发失败或销售不及预期的风险，从而对公司业绩产生不利的影响。

（二）经营风险

1、客户集中的风险

报告期内，公司销售收入客户集中度较高。公司与主要客户建立了长期稳定的合作关系，且这些客户多为信誉度较高的优质客户，但公司若不能通过技术、产品创新等方式及时满足上述客户的业务需求，或上述客户因为市场低迷等原因使其自身经营情况发生变化，导致其对公司产品的需求大幅下降，公司将面临一定的因客户集中度较高而导致的经营风险。公司的电信运营商客户为电信运营商的不同成员企业，主要签约主体为电信运营商各分子公司，单体占比集中度较低。未来，若电信运营商相关行业政策、数字化及网络安全需求出现重大变化，或公司与中国移动等电信运营商客户的合作关系出现不利变化、新客户和新产品拓展计划不如预期，可能导致公司面临收入增速放缓甚至收入下降的风险。

2、核心技术人员流失风险

经过多年积累和发展，公司形成了以核心技术人员为首的多个强有力的研发团队。为保障公司高级管理人员和核心技术人员稳定，公司制定了合理有效的股权激励机制，并同主要核心技术人员签署了保密协议和竞业禁止协议。虽然公司的核心技术并未严重依赖个别核心技术人员，但不排除掌握核心技术的部分人员不稳定，可能造成在研项目进度推迟、甚至终止，或者造成研发项目泄密或流失，给公司后续新产品的开发以及持续稳定增长带来不利影响。

3、与趋势科技合作稳定性风险

根据亚信安全（香港）与趋势澳洲签署的《知识产权许可及合作协议》和其他相关协议，公司与趋势科技目前在中国大陆地区进行独家合作，合作内容包括

趋势科技品牌产品独家分销合作、源代码合作、独家技术服务以及趋势科技品牌产品的 OEM 合作等。虽然公司自主研发能力较强，对趋势科技的依赖度有限，且公司与趋势科技已建立长期全面合作关系，但如果未来因经济形势、政治环境等原因影响，公司未能与趋势科技继续合作，仍然可能对公司短期的业务开展造成一定的影响。

4、业务协同风险

公司于 2024 年 11 月完成对亚信科技控股有限公司（以下简称“亚信科技”）的收购，亚信科技成为公司的控股子公司。公司与亚信科技在保持各自独立经营的基础上，根据实际情况及客户需求，从市场拓展、产品开发、技术研究等方面探索协同机制，在产品能力提升与融合、行业用户覆盖及深化等方面充分发挥协同效应。但是，如该等业务协同无法顺利实现，则本次收购能否达到预期效果存在一定的不确定性。

（三）财务风险

1、收入季节性波动的风险

公司通常上半年营业收入较低，而下半年（特别是第四季度）营业收入较高，存在一定的季节性特征，主要原因在于公司客户集中于运营商、金融、政府等行业和领域，这些客户往往实行集中采购制度和预算管理制度，其采购活动具有较强的季节性。许多客户在每一年的上半年对本年度的采购及投资活动进行预算立项、设备选型测试等，下半年进行招标、采购和项目建设、验收、结算，因此每年的第三、四季度往往出现收入增加的现象，可能出现不同期间营业收入波动较大的情况，存在收入季节性变动风险。

2、应收账款与合同资产余额扩大、存在坏账损失的风险

受营业收入规模增长、应收规模增加等因素的影响，公司应收账款与合同资产余额较高。未来，随着收入规模的增加，公司应收账款与合同资产余额有可能上升。如果公司延长信用期或应收款项未能及时收回，亦可能导致应收账款规模进一步扩大。如果客户信用发生变化、公司不能持续有效控制应收账款规模或及时收回账款，公司将面临一定的坏账风险，并对经营业绩造成不利影响。未来公

司将聚焦高价值客户，努力改善经营质量，持续加强回款考核管理与控制，最大程度降低坏账损失风险。

3、商誉风险

公司于 2023 年、2024 年先后完成对厦门服云信息科技有限公司、亚信科技的收购。公司始终围绕核心业务板块、从协同发展的角度选择并购标的，以求降低并购带来的风险，但并购重组也带来了一定的商誉。如果被收购企业未来经营状况出现恶化，公司则存在商誉减值的风险，从而对公司当期损益造成不利影响。公司将努力提升管理的科学性，强化并购重组后对子公司业务发展及文化融合的管理能力；针对并购重组过程中形成的商誉，公司每年会聘请专业的第三方进行商誉减值测试，如果被收购公司未来经营状况恶化，公司将及时进行商誉减值。

（四）行业风险

1、市场竞争加剧的风险

随着 5G、云计算、大数据、人工智能、物联网等技术的快速发展，公司所处行业蓬勃发展，行业应用需求呈现多样性且持续增长，行业内原有竞争对手规模和竞争力的不断提高，高端专项及复合型研发人才成为各企业激烈争夺的稀缺资源，加之新进入竞争者逐步增多，可能导致公司所处行业竞争加剧。如果公司在市场竞争中不能有效保持技术领先水平，不能充分利用现有的市场影响力，无法在当前市场高速发展的态势下扩大自身规模并增强资金实力，公司将面临较大的市场竞争风险，有可能导致公司的市场地位出现下滑。

2、行业增长速度下降的风险

随着数智化转型的深度、网络安全的渗透率日益提高，长期来讲，面临着行业增长动能减缓的情况。同时，公司的主营业务受下游行业客户 IT 投入的影响比较大，与整体的经济环境、企业盈利状况密切相关，当整体经济状况下行时，面临预算收缩的压力，行业增长速度面临下降的风险。

（五）宏观环境风险

1、产业政策变化产生的风险

国家重视信息技术及网络安全产业，并给予重点鼓励和扶植，软件与信息服务业的产业政策陆续出台。在相当长的一段时期内，国家仍将会给予信息技术及网络安全产业政策支持。如果国家对信息技术及网络安全企业的扶持政策发生变化，将对公司的发展产生相应影响。

四、重大违规事项

2024 年度，公司不存在重大违规事项。

公司在 2023 年 2 月 25 日至 2023 年 4 月 6 日期间存在使用闲置募集资金进行现金管理超出董事会授权期限的情形，公司已于 2024 年 11 月 11 日召开董事会、监事会、独立董事专门会议对相关空窗期审议追认。具体情况详见本报告之“一、保荐机构持续督导工作情况”和“九、募集资金的使用情况及是否合规”的有关内容。

五、主要财务指标的变动原因及合理性

2024 年度，公司主要财务数据如下：

单位：万元

项目	2024 年度	2023 年度	变动幅度
营业收入	359,508.23	160,808.84	123.56%
归属于上市公司股东的净利润	959.06	-29,107.58	不适用
归属于上市公司股东的扣除非经常性损益的净利润	-1,625.66	-32,494.18	不适用
经营活动产生的现金流量净额	114,541.26	-37,933.57	不适用
项目	**2024 年 12 月 31 日**	**2023 年 12 月 31 日**	**变动幅度**
归属于上市公司股东的净资产	215,416.95	211,793.85	1.71%
总资产	1,336,984.99	340,097.75	293.12%

2024 年度，公司主要财务指标如下：

项目	2024 年度	2023 年度	变动幅度
基本每股收益（元／股）	0.0248	-0.7302	不适用
稀释每股收益（元／股）	0.0248	-0.7302	不适用
扣除非经常性损益后的基本每股收益（元／股）	-0.0421	-0.8151	不适用
加权平均净资产收益率（%）	0.45	-12.03	增加 12.48 个百分点
扣除非经常性损益后的加权平均	-0.76	-13.43	增加 12.67 个百

项目	2024 年度	2023 年度	变动幅度
净资产收益率（%）			分点
研发投入占营业收入的比例（%）	15.32	27.78	减少 12.46 个百分点

1、公司 2024 年度实现营业收入 359,508.23 万元，较上年同期增长 123.56%，主要原因为数智业务加入对公司营业收入规模的提升，以及网络安全业务营业收入增长。

2、2024 年度，公司归属于上市公司股东的净利润为 959.06 万元，较上一年度扭亏为盈，扣除非经常性损益后归属于上市公司股东的净利润为-1,625.66 万元，较上一年度亏损大幅缩窄。公司利润表现上升主要系营业收入大幅上升的同时毛利水平显著提高、同时数智业务的加入使公司利润水平有所改善。

3、2024 年末，公司总资产为 1,336,984.99 万元，较 2023 年末增长 293.12%，主要系公司将亚信科技纳入合并报表范围所致。

六、核心竞争力的变化情况

（一）核心竞争力分析

1、网络安全业务

（1）数据驱动、AI原生的核心技术能力

公司自成立以来一直高度重视研发创新与管理，软件产品的技术创新、软件开发过程的改善能力、质量管理水平、软件开发的整体成熟度居于行业前列，拥有全球公认的CMMI（能力成熟度模型集成）最高等级CMMI 5权威认证。公司经过多年的探索和积累，已掌握了终端安全、身份安全、云安全、安全管理、高级威胁治理、威胁情报等领域的重要核心技术，并形成了一系列具有自主知识产权的技术成果。

公司以“数据驱动、AI原生”为核心技术理念，在北京、南京、成都设立了三大研发中心，并与国家计算机病毒应急处理中心（CVERC）在天津共建病毒实验室，共同开展高级持续性威胁（APT）方面的研究，持续为CVERC通报病毒信息；公司建成了亚信网络安全产业技术研究院，拥有网络安全态势感知中心、高级威胁调查取证中心、网络安全攻防实验室，开展前瞻性基础研究和技术创新。

公司全面拥抱大模型AI浪潮下的变革与发展，业内率先提出“AI原生”理念，致力于安全大模型与大模型安全的研究与产业化推进。2024年，在IDC《革新安全防护-基于大模型的安全能力品牌推荐与洞察——安全运营，2024》、《大模型安全检测与防护解决方案品牌推荐与洞察2024》报告中，亚信安全信立方大模型在AI与安全技术的融合与应用方面获得认可，其中告警关联、编写检测规则、引导调查、大模型攻防检测、身份识别与管理等细分领域获得推荐。

（2）能力领先、智能联动的平台化产品矩阵

公司的网络安全整体能力长期处于行业领先地位，根据安全牛《网络安全企业100强》报告，亚信安全已连续9年蝉联中国网络安全十强企业，在云安全、终端安全、身份安全等领域长期具备国内领先优势。

公司的云安全产品领先实力获得广泛认可。根据IDC的报告数据，2024年6月，在《中国私有云云工作负载安全市场份额，2023：CNAPP助力企业实现全方位云原生安全防护》中,亚信安全云主机安全产品市场份额位居第三。2024年12月，IDC发布《生成式AI推动下的中国云安全市场现状及技术发展趋势，2024》，报告聚焦于公有云场景下的安全能力，亚信安全凭借产品技术优势，成为CWPP、CSPM技术领域被推荐厂商。公司自2023年完成对厦门服云信息科技有限公司（品牌名：安全狗）的收购以来，深度融合云安全的产品技术能力，加速云原生安全创新发展，构筑完整的云安全体系。

公司的终端安全产品是一体化终端安全的引领者。根据IDC的报告数据，公司终端安全软件产品市场份额已连续多年排名第二。2024年12月，第三方机构安全牛发布《2024新一代终端安全技术应用指南暨年度Top10厂商推荐》，亚信安全TrustOne入围新一代终端安全领域十大代表性厂商。2024年9月，在Gartner《Market Guide for Zero-Trust Network Access, China》（中国零信任网络访问市场指南）报告中，公司的AISDP产品连续两年荣膺Gartner中国零信任市场代表厂商。

公司的泛身份安全类产品聚合了可信身份能力、可信认证能力、可信访问能力及合规审计能力，拥有业界先进的身份管理与认证、自适应智能身份认证、基于SIM卡的密码服务等多项核心技术，满足用户在传统IT架构、物联网、云计算、

大数据环境下的泛在身份管理需求。根据IDC的报告数据，2024年10月在《中国IT安全软件市场跟踪报告，2024H1》报告中，亚信安全身份和访问管理软件市场份额连续8年位居第一。2024年11月，在Gartner发布《Innovation Insight for Privileged Access Management in China》（中国特权访问管理创新洞察）中，亚信安全PAM产品凭借领先技术荣膺代表厂商。

同时，公司长期坚持平台化战略，基于领先产品能力，打造智能联动的XDR平台，并结合AI大模型等新技术不断创新升级，是XDR领域的领跑者。XDR整合了终端安全、高级威胁治理、云安全及边缘安全类产品能力，结合信立方大模型与云端威胁情报，通过预先精密编排的各种威胁响应预案，实现资产管理、检测分析、响应闭环、界面展示、智能运营等一体化管理，从而有效地帮助客户更早地发现威胁、更快捷地处置威胁、更便捷地修复系统，帮助客户构建全方位、智能化的平台级安全防护体系。

（3）洞察需求、精益运营的综合性解决方案能力

公司擅长为拥有大型网络和复杂IT架构的客户量身打造满足其特殊需求的综合性安全解决方案。经过多年的发展，逐步形成了涵盖身份安全、大数据分析及安全管理、5G云网边管理等多个领域的网络安全产品和解决方案体系，形成了高效的综合服务能力、项目建设能力与交付运营能力，可有效满足用户构建综合性安全防护体系的需求。

在网络架构、业务系统高度复杂、对系统稳定性、业务连续性要求极高的电信运营商和金融领域，基于对客户业务的深入理解和卓越的软件开发服务能力，公司的综合性安全解决方案得到了大量应用。公司解决方案应对大型复杂系统的安全防护能力和电信金融级别的高速响应能力经历了多年实践的检验，有效地保障了客户系统的安全性和业务连续性，得到了客户的广泛认可。

公司具备支撑国家级项目建设的工程化交付能力，可以满足大规模高稳定的复杂用户需求。公司为国务院办公厅电子政务办公室建设了国家政务服务平台统一身份认证系统，支撑全国一体化政务服务平台的统一身份互认，提供稳定的安全能力支撑。公司同时承建了国家电子政务外网安全监测平台，承担中央级政务外网数据总线的角色，对接省级外网平台，提供“威胁识别、精准监管、整体协

同、预警响应”的一体化管理能力。

（4）深耕行业、覆盖全国的专业营销与客户服务体系

公司已构建完整全面的市场营销体系，包括覆盖全国的省级办事处体系，以及深入垂直领域的行业事业部体系。在网络架构、业务系统高度复杂、对系统稳定性、业务连续性要求极高的电信运营商、金融、能源等垂直领域，基于对客户业务的深入理解和卓越的软件开发服务能力，公司的产品、平台、服务及综合性安全解决方案得到了大量应用，得到了客户的广泛认可。

作为电信运营商的长期合作伙伴，公司的产品和系统附着在电信运营商的基础网络内，覆盖了核心网、接入网和支撑网，为电信运营商提供了支撑其业务开展和运营的系统能力和安全防护，构成了电信运营商的基础网络安全能力机制；在金融行业，持续为银行、保险、证券等细分领域的客户提供终端一体化、全栈云安全防护、勒索防护与治理等产品与服务；此外，在能源、电力、制造等行业公司也在持续的拓展与深耕中获得了更多的客户认可。面对激烈的市场竞争，结合各行业客户的复杂性需求，公司通过不断提升解决方案与技术服务专业能力，加强市场与品牌推广力度，以及加强精细化管理等，持续提升客户满意度，获得客户长期认可与持续价值。

与此同时，经过多年的发展，公司形成了覆盖广泛、立体响应、及时高效的客户服务体系，形成了涵盖安全规划、安全攻防、安全评估、安全培训、应急响应等多个方面的服务能力，能够为客户提供7x24小时现场和远程支援，有效响应客户的需求，公司曾多次受邀为国家重大活动提供安全保卫服务，多次因优秀的服务表现收到相关单位的感谢函。

（5）广受认可的品牌形象与高素质人才队伍

经过多年发展，“亚信安全”已成为中国网络安全领域的领导品牌之一。公司凭借自身的产品、技术和综合服务能力优势，获得了国内外市场研究机构、政府主管部门和行业内专家和客户的认可。公司核心产品与技术以及公司市场影响力获得了国内外市场研究机构的广泛认可，在网络安全行业、身份安全、终端安全、云安全、XDR、AI+运营安全、数据安全、勒索治理、安全服务等众多领域均表现突出，奠定了在中国网络安全软件市场的领先地位。公司客户广泛分布于

电信运营商、金融、政府部委、能源等行业领域，公司的重要客户包括三大电信运营商、中国人民银行总行、五大国有银行、大型股份制银行、国家部委等重点中央部门以及国家电网、南方电网、中石化等重点企业。

公司把人才培养和组织能力建设作为一项战略投资，通过一系列有效的聘用、培养和激励机制保障团队稳定。公司对人员培养持续投入，保证源源不断的人才供给和内部人员的能力提升。公司注重管理干部的规划和建设，建立干部资源池，通过选拔、任用、培养、评估的干部管理流程，不断优化各层干部群体的知识结构和综合管理能力。公司落实优秀校招人才战略，确保形成自己的人才供应链，保障优秀校招生在中长期成为公司人才梯队的中坚力量，培养生力军。

2、数智业务

公司子公司亚信科技是国内领先的软件产品、解决方案和服务提供商，通过综合运用咨询规划、产品研发、实施交付、系统集成、数据运营、智能决策、客户服务等数智化全栈能力，为千行百业提供端到端、全链路数智化服务，客户遍及电信运营商、广电、能源、政务、交通、金融、邮政等行业。伴随技术革新发展，亚信科技正在全面拥抱AI，夯实通信行业基本盘，同时，在坚持推进三新业务发展的基础上，聚焦布局AI大模型应用与交付、5G专网与应用、数智运营三大创新增长引擎。

（1）深耕电信运营商领域，数智化全栈能力突出，AI注智显著突破

亚信科技持续深耕电信运营商领域，在BSS（Business Supporting System）和OSS（Operation Supporting System）等领域处于国内领先地位，深厚的行业积淀造就了亚信科技业内一流的数智化全栈能力，与此同时，近年来公司将“AI+”“大模型+”等创新技术引入传统业务构建了完整的AI技术应用生态。2024年亚信科技在AI注智领域取得显著突破，AI大模型相关项目总数突破新高，业务覆盖范围持续扩大。

（2）深度合作头部云计算和大模型厂商，大模型交付建立先发优势

大模型应用作为新质生产力代表，发展日新月异，正成为新兴的高增长领域，亚信科技在大模型交付业务领域起步最早、落地最快，与国内头部云计算和大模

型厂商建立了长期合作关系，在200余个项目中总结沉淀了具备核心竞争力的交付工具集合，并有每年大量各类交付业务锻炼的成熟团队和管理经验，形成亚信特色的大模型交付体系“一套规划方法+一组工具集+一支专业团队”。亚信科技通过与阿里云、火山引擎、百度智能云、DeepSeek等领先云厂商、大模型厂商的战略合作，构建了覆盖政企、能源、金融、交通等垂直领域的行业大模型端到端解决方案。2024年，已签约国家电网、中石油、南航等提供设备智能诊断、电力预测、勘探优化、财务分析等高价值场景化大模型，并在电力行业首创动态知识运营体系，实现“零训练”理解复杂业务指标、基于专家模型的成因分析等技术突破。

（3）拓展垂直行业数字化，聚焦重点行业高质量发展

亚信科技以5G、大数据、AI等创新技术赋能，聚焦能源、交通、政务等重点行业，打造行业化产品和解决方案，把握垂直行业数字化、智能化转型升级机会。亚信科技在能源行业持续深耕，构建了5G网数智一站式能力优势，推动5G专网及数智化解决方案和应用在核电、新能源、智慧风场和矿山等领域的广泛渗透。

（4）数据聚合+场景洞察+AI，具备领先数智运营能力

亚信科技数智运营业务持续深耕通信、汽车、消费、金融等行业，并作为核心ISV与火山引擎深度合作，构建基于企业微信的全生命周期私域运营平台，打造线上线下一体化运营体系。亚信科技具有“数据资源聚合+行业场景洞察+AI”综合优势，是国内按结果付费模式的领先企业。在汽车行业，为汽车出行产业链客户提供数智平台与精准营销服务，在消费行业，为多领域客户提供场景数据价值服务和数字营销系统基建，在金融行业，为客户提供数据平台和运营服务，获得广泛认可。

（5）深化研发布局，云网和数智等产品得到业界高度认可

亚信科技已形成在“云网”“数智”“IT”三大产品体系的战略布局，在技术创新和商业落地方面取得显著突破。在云网领域，5G专网产品实现国际引领，成功入围中广电移动5G ToB专网项目并成为第一中标候选人，核电行业解决方案入选OMDIA最佳实践报告，风电行业方案斩获Network X“全球最佳行业方案奖”及工信部“绽放杯”一等奖，同时创新推出基于大模型的AN Evo自智网络产

品，助力运营商网络向L4级自智化演进。在2025年3月的MWC（世界移动通信大会）上，亚信科技5G专网产品凭借优秀的产品能力和广泛的行业应用，斩获GTI Awards“最佳市场拓展与商业价值奖”（Market Development & Business Value Award）。

数智领域实现国内领先并向国际拓展，“渊思”行业大模型产品体系全面商用，构建起从国产大模型到垂直场景的完整闭环，在通信、能源、政务等领域的100余个案例中成功落地，多款产品入选Gartner、Forrester等国际权威报告，边缘智算、可信数据流通等产品加速国际化进程。

IT领域持续巩固国内第一阵营地位，PaaS平台完成AI Native重构，新增编程大模型图灵程序员和AI Infra基础设施，数字孪生、区块链等新兴技术取得突破，信创生态建设成效显著。亚信科技深度参与3GPP、ITU等9个国际标准组织工作，新增60项标准制定和202项专利，强化5G-A/6G关键技术研究，在通感算智一体化和空天地一体化方向取得重要突破，持续引领行业技术发展，为全球通信行业贡献创新力量。同时正式加入AI-RAN Alliance，全面推动人工智能（AI）与无线接入网络（RAN）和5G OSS深度融合，共同构建无线通信面向Open AI Native的未来。

3、安全+数智一体两翼，形成云网安一体化综合能力

中国数字经济蓬勃发展，云计算和网络成为新一代数字经济底层基础设施，AI新技术、新应用快速演进，数据要素重要性日益凸显，伴随着用户新场景、新业务、新标准的涌现，需要行业内企业通过持续的新技术运用和新产品的研发以满足用户需求。同时，数智化系统承载并处理大量的用户、业务等高价值数据，其稳定性、安全性和响应速度要求较高，对行业内企业的技术能力要求越来越高。因此，“云网安”融合将成为大势所趋，安全+数智一体化的综合服务能力将成为软件企业的核心竞争力。

凭借亚信安全自身在“安全”领域的突出优势，以及子公司亚信科技在“云”和“网”领域的深厚积淀，公司将进一步打造“懂网、懂云、懂安全”的能力体系，构建云网安一体化的核心竞争力。在市场协同方面，加强双方在均具备优势的电信运营商领域的协同深耕，提升面向客户的解决方案完整性与领先性；在产

品与技术方面，结合双方在网络安全、大模型、数据要素、5G专网、云计算等领域的技术优势，联合发力，形成覆盖“云网安”的全场景业务体系，形成强强联合的协同力与市场竞争力，实现长期共赢。

（二）核心竞争力变化情况

公司于2024年11月完成对亚信科技的非同一控制下的控股合并。亚信科技的加入，扩大了公司的业务范围，丰富了公司的产品结构，未来，公司业务体系主要由网络安全业务、数智业务两大板块构成。如上文所述，公司将新增数智业务方面的核心竞争力，并通过将数智业务与网络安全业务的融合，打造安全+数智一体化的综合服务能力，形成覆盖“云网安”的全场景业务体系，形成强强联合的协同力与市场竞争力，实现长期共赢。

七、研发支出变化及研发进展

（一）研发支出及变化情况

2024年度，公司研发费用为5.41亿元，公司研发投入占营业收入的比例为15.32%，与2023年度研发费用率27.78%相比，减少12.46个百分点，主要系公司于2024年11月起将亚信科技纳入合并报表范围后，营业收入大幅增长。公司的研发投入的情况如下表所示：

单位：万元

项目	本报告期	上年同期	变动幅度
费用化研发投入	54,066.47	44,672.56	21.03%
资本化研发投入	997.66	-	不适用
研发投入合计	55,064.13	44,672.56	23.26%
研发投入总额占营业收入比例（%）	15.32	27.78	减少 12.46 个百分点
研发投入资本化的比重（%）	1.81	-	增加 1.81 个百分点

（二）研发进展

2024年度，公司主要在研项目具体如下：

单位：万元

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
网络安全业务	1	海鸥威胁行为检测引擎（AttackIO）	1,800	572.39	1,058.36	相关产品已进入市场，目前已获得客户认可。	基于 ATT&CK 模型利用 AI 算法，构建高精度的行为检测引擎。依托 Agent 端收集、研判、聚合受保护主机日志，产生战术点告警事件；依托云端聚类、降噪、关联产生杀伤链告警。使用户摆脱告警风暴，并了解攻击路径和应对方法。云端引擎具备学习能力，以应对不断变化和增长的网络攻击方法。	具备未知威胁检测能力；检测规则覆盖 14 个战术点，及超过 400 个黑客攻击技术点，达到行业先进水平；检测规则数量超过 2400 条，为覆盖更多 ATT&CK 技术点，持续增加中；与云端分析引擎互动，进一步提高检测能力。	可应用于网络安全行业，对安全有较高要求的企事业单位，与传统安全引擎形成纵深防御体系,解决系统中存在的安全问题。
	2	梦蝶文件防病毒引擎（MalDetect）	3,500	572.39	2,789.16	相关产品已投入市场，目前已获得客户认可。	新一代的轻量级文件防病毒引擎，增强对新型威胁的检测能力，如国产化平台病毒，WebShell、无文件攻击、勒索、银狐木马等热门威胁的检测。	新一代文件防病毒引擎融合了特征码、云查杀、启发式、机器学习及其他新型检测技术，以海量样本威胁数据作为支撑，并构建起小时级的威胁发现、反馈和全网免疫闭环通道，具备强大的对未知威胁的检测能力。	可广泛用于对安全有较高要求的关键基础设施行业，为自研安全产品提供基于静态文件病毒的检测与阻断。
	3	怒狮网络威胁检测引擎	3,300	685.43	2,882.24	相关产品已进入市场，目前已获得	新一代高性能的网络威胁检测引擎，适配主流平台及国产化系统，满足产品	已知威胁覆盖全面，有效发现真实攻击，内置 10+机器学习模块，80+深度研判模块，对于多种攻	可广泛用于对安全有较高要求的关键基础设施行业，为自

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
		（NetStack）				客户认可。	的定制化需求，持续增强网络威胁的检测能力，加强新型漏洞的查杀能力。	击技术点深度研判;具备0Day漏洞的检测能力和新兴攻击技术的检测能力。	研安全产品提供基于网络流量的检测与阻断。
	4	魔龙盾威胁指标评估引擎（Maldium）	2,300	414.98	1,888.53	相关产品已进入市场，目前已获得客户认可。	基于数据湖海量威胁情报数据以及亚信安全的“智能防护网络”云端研判服务，构建高性能威胁指标评估引擎提供 Web 信誉、失陷指标检测、勒索风险预警能力，增强网关、APT及终端类产品威胁检测能力，形成了情报运营闭环。	亚信安全基于底层数据湖威胁情报，依托蜜罐云、沙箱云、网络测绘技术手段，通过深度学习、数据挖掘、专家规则等近百种情报生产模型和算法用于情报生产、研判。利用反馈机制辅助修正保证情报强时效、高精准与低误报；引擎端内置多种缓存机制，本地缓存机制与云端联动机制，在产品的威胁检测能力极大提升的同时,也保证了高检测性能；在 Web 信誉、失陷指标检测、勒索风险预警能力在业界处于一流水平。	魔龙盾威胁指标评估引擎，可以为云安全、身份安全、终端安全、安全管理、数据安全、高级威胁治理等各类安全产品提供高质量的情报评估服务。适用于运营商、金融等多种行业和场景。
	5	亚信安全威胁数据湖（AIS-TIDL）	3,300	414.98	2,944.86	项目正处于相关模型与关键技术的持续迭代阶段	广泛收集内外部威胁数据，包括开源情报，付费情报，反馈情报与合作情报，利用大数据技术妥善保存和管理威胁情报，沉淀亚信安全在威胁情报领域的数据资产。针对多源异构情报进行数据标准化，形成情报元数据库，面向各类应用场景构建数据资产目录，使得数据成为公司	已集成上百家以上情报源，包括战术级情报源与战略级情报源；已积累有效威胁数据，互联网类超过 120 亿，文件类超过 20 亿；已集成自动化分析流程超过 20 个，文件类情报更新频率小于 4 小时，互联网类情报更新频率小于 1 小时；数据资产目录达 100 个。	赋能 XDR 平台，提升威胁治理能力，最终达到全网免疫能力。

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
							显性核心资产。		
	6	一体化终端安全平台研发	9,000	2,684.25	5,822.36	相关产品已投入市场，目前已获得客户认可。	终端安全防护平台组件管理框架能力持续提升，增强产品平台管理能力；优化高级威胁终端检测与响应系统资产管理功能，完善 EPP+EDR+资产管理方案；更新核心引擎，增强防病毒能力；提升无文件攻击检测能力；增强机器学习的本地模式，强化用户在无法连接到互联网时也可以得到机器学习的保护能力。	基于下一代终端防病毒技术，利用机器学习，行为监控，云查杀和传统特征库结合的方式，有效防范恶意威胁软件、勒索病毒、挖矿软件等已知和未知威胁，同时插件化的方式构建终端安全一体化平台，全面覆盖威胁防御和终端安全管理，支持大规模分级部署，并可与第三方管理平台集成实现统一管理和态势感知。	广泛用于对安全有较高要求的金融、高端制造和关键基础设施等行业，为用户提供终端安全防护平台化和整体性解决方案。
	7	高级威胁发现与分析平台研发	7,500	1,668.84	6,840.21	相关产品已投入市场，目前已获得客户认可。	增强网络内容检测引擎能力，提升网络流量解析及网络流量威胁检测性能；增强网络文件内容恶意行为分析引擎能力，提升网络文件内容深度扫描和检测性能；提升沙盒检测能力，提升对 APT 攻击的动态分析检测能力；增强以失陷资产为核心的威胁关联分析和威胁溯源能力。	能侦测所有端口及 100 多种通讯协议的应用，用规则引擎、威胁情报、机器学习、沙箱动态模拟分析等技术，能快速发掘并分析恶意文档，恶意软件、恶意网页，违规外联、勒索软件以及传统防护无法侦测到的内网攻击以及定向 APT 攻击活动。	可广泛用于对安全有较高要求的金融、高端制造业等客户，为客户提供业界领先的 APT 检测和分析能力，帮助客户应对日益变化的攻击场景，提供持续的防护。满足基于等保合规和客户实际需要的网络边界防病毒需求，聚焦的行业包括政府、小金融、制

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
									造业。
	8	DNS 域名解析产品研发	5,000	1,008.58	3,518.42	相关产品已进入市场，稳定开发优化阶段。	提高产品高并发处理能力，降低缓存响应时延，保持 DNS 产品市场领先性；持续增加产品的国产化适配能力，增强市场竞争力。	域名解析产品可支持缓存超过 4000 万条域名记录，在高并发处理场景下，DNS 缓存应答处理时延低至 1ms 内；对主流国产芯片的兼容，产品同时进行了 X86 和 ARM 架构的兼容适配，保证了高性能解析技术在不同硬件架构下都能达到较高的性能水平；对主流国产操作系统的兼容，产品进行了国产操作系统龙蜥、欧拉、CTyunOS 的兼容适配，提升了国产化适配能力；基于全新设计的框架，引入新的策略处理机制、策略匹配算法，减少内存资源占用，提升冷加载速率。	DNS 全业务域名解析系统已经部署全国 20 多个省级运营商，为数亿手机和家宽用户提供安全、快速、稳定、智能的域名解析服务，支撑互联网业务发展。
	9	安全运营及态势感知平台	8,800	890.06	8,477.03	相关产品已投入市场，目前已获得客户认可。	升级现有产品的架构，提高系统的可扩展性和性能，增强生态兼容能力，满足集群化部署和节点可扩展。系统处理性能和第三方设备的对接能力达到业内前列。发布支持国产化操作系统的产品。	具备亿级以上数据量秒级统计、查询、展示能力，支持大数据+分布式架构，硬件化部署，支持横向扩展；单服务器处理能力达到 2 万 EPS，3 节点集群处理能力达到 4 万 EPS；已完成 150 余款第三方安全设备与十余款自有安全产品的联动处置响应对接；具备基于 BI 能力的工作台和报告生成；支持麒麟、统信、欧拉等操作系统。	提供安全顶层聚合能力，以 AI 和大数据分析为支撑，以主动防御为核心，建立安全数据汇聚、检测预警、分析研判、协同防御、安全可视于一体的安全运营和态势感知中心。产品应用于政府、金融、运营商、公安、企业

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
									等行业单位。
	10	零信任产品研发	4,000	328.34	3,242.10	相关产品已进入市场，稳定开发优化阶段。	以 SDP 为关键组件，统一身份，以 AI 智能可信分析决策引擎为大脑，融合终端安全，形成亚信安全的零信任安全架构体系，同时联动态势感知、威胁引擎，基于零信任身份，贯穿“云、网、端”全域全流程安全业务访问，实现持续信任评估，安全动态的访问控制，全面保护业务安全。	通过隐身网关、WEB 网关、隧道网关、控制中心、持续信任评估引擎、访问控制引擎等核心组件，融合终端安全能力，实现身份可信识别能力、持续信任评估能力、网络访问控制能力、应用访问控制能力和全面安全防护及可视化能力。	满足企业远程安全办公、多云多数据中心安全访问、终端安全一体化等场景需求。
	11	运维安全管理与审计系统	3,300	441.36	2,861.66	相关产品已投入市场，目前已获得客户认可。	迭代升级技术架构，增强安全能力，支持联动登录能力，扩充管理端国产化整体兼容性，提升产品整体交互体验。	通过运维协议代理网关，应用发布网关来提供运维用户全生命周期管理，运维访问控制细粒度授权与命令控制、对运维资产和应用工具集中管理、单点登录、操作日志录像关联审计；提供运维文件传输病毒防护能力。	辅助企业完成等级保护等法令法规对企业运维的合规要求，并提供验证，授权等账号资源管理功能的统一安全运维管理方案，满足本地运维管理、混合云安全管理、密评检测场景需求。
	12	网络威胁入侵防护系统	4,000	1,282.20	3,743.77	相关产品已进入市场，稳定开发优化阶段。	在确保高吞吐、低时延的条件下，对网关侧流量进行实时检测和分析，能够根据需要对威胁流量进行阻断和通知终端客户，而	基于高级威胁扫描引擎以及文件高速还原技术，支持 HTTP、FTP、SMTP、POP3、SMB(v3)等超过 100 种协议的识别、分析和扫描，具备业界领先的虚拟补丁	广泛用于对安全有较高要求的金融、高端制造、政府等关键基础设施等行业，为用户提供网关侧病

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
							且相关技术能够不断迭代和更新，能够对新型的威胁攻击如勒索等事件进行防护。此外，系统需要具备很高的稳定性，提供各种方式便于管理和运维，具备较高的开放性，能够和其他威胁检测和防御产品协同作战，为客户提供威胁立体防御能力。	技术，能够对网络入侵威胁事件进行实时、有效的拦截；高并发、高性能网络流量处理技术，综合威胁检测和防御吞吐能力达到了 20G 以上。	毒防护以及漏洞利用等入侵威胁防护整体性解决方案。
	13	信舱共享免疫 SaaS 系统	4000	1,467.26	3,336.13	相关产品已投入市场，目前已获得客户认可。	通过 EDR/XDR 检测手段结合威胁情报、云沙箱和威胁图，能够有效检测传统防病毒无法检测到的真实威胁；为客户提供 7*24 的托管运营服务，对真实威胁实现“早发现”、“早诊断”和“早处置”，领先攻击者一步抵御高级威胁。	目前已覆盖超过 360 个 ATT&CK 技术点，结合威胁情报、云沙箱和云端威胁狩猎，以异常行为检测来帮助用户发现传统防病毒检测不到的真实威胁；通过失陷 IOC 特征库（超过 200 万条）检测用户环境中的 C&C 连接，以数据驱动 AI 原生的方式提升 7*24SOC 服务的效率，达成一地检测、全网免疫的防护效果。	广泛应用于制造、金融、能源和运营商等行业客户，通过 7*24 的托管运营服务让客户以更好的性价比来享受安全专家服务，以 EDR 为核心构建 XDR SaaS 平台，通过云端威胁狩猎检测到专业黑客团伙的入侵攻击，通过 AI 达成降噪和提纯的效果，提供更加精准的真实威胁检测和响应服务。
	14	云原生安全(容器安全)	10,500	5,242.34	7,889.48	相关产品已投入市场，目前已获得	在云原生场景下，通过一个“N 合 1”安全基座，以工作负载为中心构建覆盖宿	创新实现镜像分层扫描能力，达到镜像间的相同层不重复扫、支持按照镜像画像标签作优先级	可广泛应用于公有云、私有云和混合云场景，在守护央企、

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
						客户认可。	主机安全、容器安全、网络微隔离和云原生态势感知全栈安全需求的一站式平台，可以支撑满足具有“高度监管、技术安全性和稳定性要求严苛”的关键信息基础设施高级云原生安全场景需求。	排序，提升镜像扫描效率 5 倍以上；支持常见的国产信创操作系统镜像（Neokylin、OpenEuler、Anolis、UOS、BC-Linux、alibaba cloud Linux）、信舱中间件镜像的扫描检测和运行时容器安全防护；容器模式部署支持非特权，不再挂载主机敏感目录。	运营商、金融和大型企业的业务环境安全中发挥着较大作用，主要目标客户群体为金融、运营商、云计算服务商、5G MEC 边缘云、政府、医疗、教育、中大型企业等行业客户群体。
	15	大模型安全与管控	6,000	3,673.77	4,096.95	通过概念验证，目前处于持续迭代阶段。	针对大模型的安全风险，提供端到端的安全防护策略，从数据清理、模型训练、微调、推理到大模型部署，线上运营监控等所有环节进行安全评估和实时监控。	提供大模型幻觉检测、训练数据投毒、提示词注入攻击、模型对抗攻击、越狱攻击、模型萃取攻击、法律法规风险等主要安全风险监测和防护能力。	应用于大模型私有化部署场景，例如金融、运营商等行业。
	16	外部攻击面管理平台	6,000	2,068.17	2,068.17	相关产品已投入市场，目前已获得客户认可。	打造一款基于攻击视角下的自动攻击弱点发现及轻量化渗透的平台。同时在易用性上实现一键任务下发、报告导出即交付，快速帮助防守方理解并及时收敛攻击风险，提升防御能力。	具备本地化部署、SaaS 两种服务方式；互联网资产检测覆盖 8 种线索，10000+产品指纹，具有影子资产、暴露面检测能力；商业泄密检测覆盖 40+网盘、文库、代码托管数据源，累计 3000+数据清洗规则，检测准确率行业内 TOP3。	广泛应用于实网攻防演练前的暴露资产摸排；多分支集团企业的日常常态化运营；监管单位对于区域/行业的内各重点企业的监督管理几个场景。
	17	数据安全与治理平台	5,000	4,385.59	4,385.59	相关产品已进入市场，稳定开发优	以数据安全大数据分析为支撑，以数据安全全生命周期管控为核心，以数据	数据资产梳理支持扫描传统关系型数据库/表/数据资产，至少支持 mysql、oracle、greenplum，	广泛应用于运营商、金融、能源和医疗等行业客户，除单机部

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
						化阶段。	安全策略统一管控为抓手，构建集资产梳理、数据接入、分析研判、响应处置、安全可视于一体的数据安全运营平台，实现全域风险感知、自适应安全闭环。	达梦(dm)16 种类型；数据资产梳理支持扫描大数据存储组件存储的数据资产，至少支持 hdfs,hive 等 6 种类型；数据分类分级支持基于 Aho Corasick 自动机实现的多模式字典匹配算法，实现高效的字典匹配识别能力。	署，DSOP 还支持集群化部署，横向提供产品采集、分析等能力，满足大规模分析的场景。
	18	身份安全管理与认证系统	6,800	5,519.57	5,519.57	相关产品已进入市场，稳定开发优化阶段。	将 AI 智能体技术应用于 IAM（Identity and Access Management，身份与访问管理）产品，旨在通过智能体的感知环境、推理分析、自主行动、做出决策并与环境交互的能力，来优化和提升 IAM 系统的功能和用户体验。智能体规划方向包括智能化身份认证、异常行为监测与响应、智能授权策略、智能化访问控制策略、自动化威胁检测与响应、响应零信任安全策略、增强用户体验、身份数据保护、合规性检查、智能客服与帮助、风险评估等领域	已发布智能体开发平台：对接公司的信立方大模型、国内主流的开源大模型和中国移动客户化大模型深瞳；智能体编排能力：除了自身提供的智能体编排能力，还兼容各运营商智能体编排系统和平台，为智能体的设计、研发、迁移和运营提供了保障；RAG 知识库开箱即用：支持内置语料，提供知识库从创建、语料录入到语料向量化、检索、总结等各方面能力，为智能客服场景提供了有力的支持。	在运营商等行业落地以下场景：智能客服，帮助用户快速获得身份安全垂直行业的业务知识以及平台功能使用方面的常见 FAQ 知识，提升用户效率和使用体验；智能身份管理：基于用户行为分析用户风险，动态调整用户多因素认证策略，提升安全性；AI 驱动的风险检测和安全审计：利用大模型实现智能检测、行为分析和自动化审计，提高效率和安全管控；在运维监控平台利用 AI 大模型进行异常日志解读，

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
									辅助用户快速定位故障根因。
	19	终端安全立体化防护平台	3,000	2,684.25	2,684.25	相关产品已进入市场，稳定开发优化阶段。	基于终端安全，融合身份安全，业务安全，数据安全，构建立体化防御体系；基于身份的安全管理体系，构建基于身份的从终端、访问控制、数据安全的安全策略管理中心；平台化管理，基于平台，统一管理防病毒、EDR、运维管控、零信任、准入、DLP、数据沙箱等不同组件；统一客户端，融合各个功能模块、形成简单易用的融合终端。	融合 CTEM 技术、零信任技术、数据沙箱技术，通过精密编排各个功能组件，层层收敛，有效降低威胁可以入侵的暴露面。在威胁防御方面，通过防病毒和 EDR 结合，基于行文分析引擎、机器学习引擎、Att&CK 检测技术、关联分析算法，可以精准发现已知和未知威胁，帮助企业有效抵御勒索攻击和银狐木马攻击。病毒防护特征库已累积 10 亿量级，PE 类检测率达 98.6%。攻击行为检测规则数量 1000 条以上，技术点覆盖度达 70%。精准检测银狐木马，防病毒检测率达 94.9%，行为规则 100%覆盖银狐攻击常用攻击手法。通过终端各类风险感知技术和零信任动态评估技术结合，进一步帮助企业提升威胁防御的效果。在数据安全方面，通过 DLP 技术、数据沙箱技术，叠加零信任技术，建立安全业务空间，有效避免数据泄露。	广泛用于对安全有较高要求的金融、高端制造和关键基础设施等行业，为用户提供终端安全勒索防护深度治理整体性解决方案。
数智业务	1	5G 网络自智平台研发项目	4,849.39	747.02	4,314.17	相关产品已进入市场，稳定开发优	进一步提升网络产品的智能化水平和自动化能力，实现网络运维的全流程智	功能升级：基于大模型技术，通用人工智能与认知增强平台，智能体平台底座基础，新增了网络	运营商市场：面向网络高价值场景向自智网络 L4 演进的场

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
						化阶段	能辅助，实现与多个省份的运营商客户达成合作与产品落地。	增强实时分析、网络运维知识问答等 7 个自智网络副驾工具，涵盖了网络运维，网络故障定位、投诉处理等多个专业场景，初步实现了网络运维的智能化辅助。技术架构升级：采用业界成熟、开放的技术框架，如 Docker 容器引擎、Kubernetes 容器管理和编排、Antdb 国产数据库等，提升了系统的处理效率、灵活性和可扩展性。	景。帮助运营商提高网络运维效率、优化网络性能、提升用户体验。
	2	5G 行业专网产品研发项目	5,132.39	927.22	5,127.70	相关产品已进入市场，稳定开发优化阶段	产品能力持续增强，在国内相关领域达到技术、市场份额国内领先。	版本持续演进：发布了全新的 3 款专网交换机、3 款专网智联网关、3 款 5G CPE 等网元/硬件。实现了端到端产品适配，可有效支撑垂直领域客户。功能升级：发布了包括了 TSN（时间敏感网络）、LCS（高精定位）、RedCap（轻量化 5G）、算力内生 Phase3、解决超远覆盖无线 Relay、专网一站开通部署等特色功能。产品获得工信部入网证，并荣获多项国际奖项与荣誉。	产品在国内核电领域已有规模部署，仍有一定市场空间；在风电、光伏等新能源场站有较好应用前景；在井工矿内巷道、矿外通信有较好应用前景；在工业、教育、港口等领域也有较大应用空间。
	3	自服务智能 PaaS 平台研发项目	2,210.87	327.44	2,063.86	相关产品已进入市场，稳定开发优化阶段	构建技术中立、生态融合、灵活组装、AI 赋能的自服务智能化 PaaS 平台，赋能企业数智化转型。	重点完成了轻量化、AINative 化、技术组件标准化改造，中间件国际标准跟进，打造了统一智算基础设施管控平台，并提供云成本分析优化等增值能力。	产品在大模型私有化云原生部署，智算资源统一管理调度，云成本优化分析、绿色计算，国产中间件

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
									替换具有广阔的应用场景。
	4	通用大数据基础平台研发项目	4,236.15	755.55	3,785.57	相关产品已进入市场，稳定开发优化阶段	聚焦企业数据要素，提供海量多模数据存储与离在线一体数仓，支撑批流数据处理，满足多业务场景大数据分析需求，助力企业打造高效、安全、稳定的通用型云原生数据技术底座。	湖仓存储引擎：新增安全访问服务和表服务，解决表数据访问安全问题，满足对外开放集成和表授权的能力。实时分析引擎：引入 Doris 满足实时秒级的实时指标计算分析能力，支撑低延迟类业务场景。存储加速引擎：增加基于策略的数据迁移功能，提高存储集群的经济化管理能力，显著降低存储成本。虚拟访问引擎：屏蔽异构和分散的物理数据源，提供统一的数据访问、权限管控、集成编排和元数据采集服务。	满足垂直行业“自主可控”的数字化要求，能够为其提供安全稳定、生态开放的大数据存储与计算底座，具备广阔的应用前景。
	5	企业级大模型开发平台研发项目	6,123.81	1,176.87	5,881.36	相关产品已进入市场，稳定开发优化阶段	为企业智能化转型提供一站式的行业大模型开发平台	面向大模型领域，纳管 100+大小模型资产，6 步即可构建行业大模型，支持大小模型协同学习。产品技术先进性获全球认可，入选 Gartner 魔力象限"领导者"象限。	涵盖通信、能源等多个行业，覆盖行业大模型开发、AI 小模型开发等多个场景，已形成 10+行业最佳实践案例。
	6	统一智能研发运维平台研发项目	1,641.15	257.67	1,536.42	相关产品已进入市场，稳定开发优化阶段	在研发各环节引入大模型技术，提升开发效率；在运维领域打造一个跨行业、智能化的统一可观测性平台，保障业务稳定运行。	研发领域：具有基于编程大模型的代码检索、代码解释、代码生成等能力，并进行低码&有码相融合、低码多语言、多组件能力完善等。运维领域：具有对采集客户端标准化打造，并完善和补	重点应用于大型企业软件研发智能化与 IT 系统一体化运维可观测场景。

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
								齐移动端可观测、大模型可观测及前后端全链路可观测等能力。	
	7	数字孪生产品研发项目	1,347.33	297.91	1,480.69	相关产品已进入市场，稳定开发优化阶段	实现数字孪生场景低成本高效率构建、业务流程智能化编排以及更智能化的部署和运维，满足跨行业（如城市规划、智能交通）的高精度可视化以及实时数据分析需求。	完成以 NeRF 三维实景重建技术为代表的空间智能能力建设，通过消费级无人机或手机拍摄的图片/视频，基于 3DAIGC 生成式建模能力快速构建高精度三维实景模型，在提升整体模型质量同时大幅降低场景建模门槛和建设成本；构建了对话式孪生场景构建能力，依托大模型语义理解能力，实现用户通过自然语言交互快速生成定制化数字孪生场景，提升场景搭建效率；自研了双引擎融合技术，单代码库适配 Web 端与 UE 引擎场景构建，实现"一次开发、多端复用"，降低开发成本与周期。	城市规划：快速构建城市数字底座，支持交通模拟、灾害推演等场景。交通治理：搭建智能感知网络，实时监测车流态势，动态优化信号配时与路径规划。应急指挥：多维构建灾害数字模型，支撑风险预警、预案联动推演与救援资源精准调配。工业制造：实现产线全生命周期监控与工艺优化，提升生产效能。智慧园区：融合 IoT 数据构建管理孪生体，优化资源配置与应急响应。
	8	AntDB 超融合数据库研发项目	3,965.27	460.34	2,997.94	相关产品已进入市场，稳定开发优化阶段	构建自动化、平台化、智能化的超融合架构通用型数据库，覆盖传统交易分析、高性能内存、流处理和时序等 5 大用户场景；增强对外开放共享能力，实现数据共享与价值提升；提	构建自动化、平台化、智能化的通用型数据库，实现分布式数据库的超融合再进化；搭建流式处理引擎、多存储引擎基础架构；软硬件深度融合国产生态适配；实现了智能化可视化的全生命周期运维管控。	覆盖通信、金融、能源、党政、交通等行业。包括存量市场进行 DB2、O 库的替换和开源数据库方案的升级，以及其他行业的数据库国产化

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
							供统一数据库开发平台工具等。		替代。
	9	营销服数据智慧共享中心研发项目	896.79	171.86	631.11	相关产品已进入市场，稳定开发优化阶段	进一步提升产品的智能化水平和自动化能力，降低系统故障，提升系统算力，减少硬件投资、缩短故障恢复时间；通过运维智能问答和参数配置助手给运营注智，提升运营效率，提升数据准确性；汇聚并治理 BSS 域内的海量数据，通过高效的整合与加工处理，对外提供全面融合且实时的数据服务能力。	通过智能问答与自动回复处理客服问题，学习文档数据并推理，提供运维策略、资源优化及故障解决建议（计费智库）；支撑使用者可通过多轮对话，系统自动解析使用者意图生成和展示各类统计数据和图表。对销售品配置数据进行多维度稽核（如完整性、影响范围等），解决复杂关系型数据库中数据关联混乱、影响范围难追溯的问题，以提升数据管理效率。技术架构上全面采用去 O 架构方案、引入实时流数据处理、AI 大模型领域、知识图谱等相关技术组件。	运营商新业务计费支撑、一点结算，计费智能调度等要求；各类服务专区场景，
	10	政企客户全业务智慧运营平台研发项目	2,021.11	390.32	1,411.70	相关产品已进入市场，稳定开发优化阶段	实现政企客户业务办理的全流程自助化、智能化，提升业务办理效率和客户满意度；推动营业厅从传统受理向营销+受理转型；优化产销品管理，缩短产品上市周期，提升运营效率。	选型业界领先的大数据互联网化资源管控架构，运用 hadoop,k8s,Mesos,yarn 等互联网资源管控技术构建查询中心的动态高可用架构；落地大数据开源软件+传统数据库的混搭架构，组合传统关系型数据库和 hbase，flink 等多个主流大数据组件，对查询数据进行温控，全方位提升客户体验。以构建智能交互、智能感知、智能空间服务为	可广泛应用于运营商的营业厅业务办理、政企客户服务、产销品管理等场景。

业务板块	序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
								交互载体，基于数智底座，通过 AI 和数据中枢统一调度微分化业务能力，构筑全方位 AI 原生业务支撑体系。	
	11	智慧园区综合管控平台研发项目	1,241.47	127.27	749.02	相关产品已进入市场，稳定开发优化阶段	与各地平台公司合作推广落地到各地化工园区及煤矿集团。	产品技术架构采用业界成熟、开放的技术框架，Docker 容器引擎、Kubernetes 容器管理和编排、等，提升了系统的处理效率、灵活性和可扩展性。	化工园区：安全管控，提升安全管理效率；精准识别与评估风险；强化应急管理能力。煤矿综合管控：形成矿山数据感知、互联、分析、自学习、预警、决策、控制的完整智能系统，以实现矿井开拓、采掘、运通、洗选、安全保障、生态保护、生产管理等全过程智能化运行。
	12	云网服务编排研发项目	75.99	13.41	43.53	相关产品已进入市场，稳定开发优化阶段	利用编排引擎新建诊断和处置流程模块，诊断流程用于诊断和发现卡单问题的根因，实现自动化处理；借助 RPA 机器人技术，辅助模拟编排流程的关键操作，减少人工的介入，提升卡单自愈率。	初步建设了 AI 智能助手卡单处理能力；基于副驾产品的本地知识库构建+集团知识图谱和启明大模型应用构建了两级卡单运维处理体系.	应用于运营商卡单的自主分析决策和多系统能力协同自主调度等场景。
/	**合计**	/	**130,841.72**	**41,657.63**	**106,071.91**	/	/	/	/

八、新增业务进展是否与前期信息披露一致（如有）

不适用。

九、募集资金的使用情况及是否合规

（一）实际募集资金金额、资金到位时间

根据中国证券监督管理委员会于 2022 年 1 月 5 日出具的《关于同意亚信安全科技股份有限公司首次公开发行股票注册的批复》（证监许可[2022]7 号），公司启动发行工作，向社会首次公开发行人民币普通股（A 股）股票 4,001 万股，每股发行价格为人民币 30.51 元，募集资金总额为人民币 1,220,705,100.00 元，扣除发行费用人民币 98,199,233.77 元（不含增值税金额）后，实际募集资金净额为人民币 1,122,505,866.23 元，上述募集资金已经全部到位。致同会计师事务所（特殊普通合伙）对本次公开发行新股的募集资金到位情况进行了审验，并于 2022 年 1 月 28 日出具了《验资报告》（致同验字（2022）第 110C000069 号）。

（二）2024年年度募集资金使用及结余情况

截至 2024 年 12 月 31 日，公司已累计投入募集资金总额 1,204,115,378.52 元，募集资金余额为 56,030,774.62 元（包括累计收到的银行存款利息、理财收益扣除银行手续费），其中用于现金管理 50,353,910.44 元，募集资金账户余额为 5,676,864.18 元。具体情况如下：

项目	金额（元）
募集资金总额	**1,220,705,100.00**
减：已累计投入募集资金总额	**1,204,115,378.52**
2022年度募集资金置换预先投入自筹资金部分	-
2022年度投入募集资金用于支付承销费、保荐费（不含税金额）	73,242,306.00
2022年度投入募集资金用于支付其他发行费用（不含税金额）	22,906,927.81
2023年度投入募集资金用于支付其他发行费用（不含税金额）	2,049,999.96
截止本报告期末累计募投项目支出	**1,105,916,144.75**
其中：2022年度募投项目支出	330,982,193.64
2023年度募投项目支出	564,610,326.98
本期募投项目支出	210,323,624.13
加：利息收入	**7,958,353.96**

项目	金额（元）
其中：以前年度利息收入	7,859,825.76
本期利息收入	98,528.20
加：理财收益	**31,499,016.72**
其中：以前年度理财收益	28,935,123.99
本期理财收益	2,563,892.73
减：手续费支出	**16,317.54**
其中：以前年度手续费支出	14,765.09
本期手续费支出	1,552.45
减：募集资金结项永久补充流动资金	**-**
募集资金余额	**56,030,774.62**
其中：暂时闲置资金进行现金管理投资	50,353,910.44
结构性存款	50,000,000.00
协定存款	353,910.44

（三）募集资金的管理情况

公司对募集资金采取专户储存制度，并与保荐机构、存放募集资金的开户银行签订了募集资金监管协议。

2022 年 3 月 11 日，公司召开第一届董事会第十一次会议、第一届监事会第九次会议，审议通过了《关于调整募投项目拟投入募集资金金额及新增募投项目实施主体并使用部分募集资金向全资子公司增资以实施募投项目的议案》，为顺利推进首次公开发行股份募集资金投资项目（以下简称“募投项目”）的实施，同意公司根据首次公开发行股份募集资金实际情况，对募投项目使用的具体募集资金金额进行调整，同意增加亚信科技（成都）有限公司作为募投项目的实施主体，并通过南京亚信信息安全技术有限公司向亚信科技（成都）有限公司增资 92,000 万元的方式具体实施。

2022 年 6 月 24 日，公司召开第一届董事会第十三次会议、第一届监事会第十一次会议，审议通过了《关于使用募集资金置换已支付发行费用的自筹资金的议案》，同意公司使用本次发行募集资金置换已使用自筹资金支付的发行费用合计 14,889,946.64 元。

（四）募集资金使用的其他情况

2022 年 2 月 25 日，公司第一届董事会第十次会议、第一届监事会第八次会议分别审议通过《关于使用部分暂时闲置募集资金进行现金管理的议案》，同意公司使用最高不超过人民币 10.10 亿元（含本数）的暂时闲置募集资金进行现金管理，使用期限为自董事会审议通过之日起 12 个月内，在前述额度及期限范围内，资金可循环使用。2023 年 2 月 25 日，董事会决议期限届满，公司未能及时赎回 5.65 亿元闲置募集资金购买的理财产品。2023 年 4 月 7 日才召开第二届董事会第十八次会议、第一届监事会第十六次会议，分别审议通过《关于使用部分暂时闲置募集资金进行现金管理的议案》，同意公司使用最高不超过人民币 6.8 亿元（含本数）的暂时闲置募集资金进行现金管理，使用期限为自董事会审议通过之日起 12 个月内，在前述额度及期限范围内，资金可循环使用。在 2023 年 2 月 25 日至 2023 年 4 月 6 日之间，公司闲置募集资金进行现金管理存在授权空窗期，在闲置募集资金现金管理授权空窗期内无新增购买的理财。

因前述事宜，江苏证监局对公司、时任财务总监出具警示函措施。2024 年 11 月 15 日，公司召开第二届董事会第十五次会议、第二届监事会第十三次会议、第二届董事会独立董事 2024 年第十一次专门会议，审议通过《关于追认使用部分暂时闲置募集资金进行现金管理的议案》，就公司使用闲置募集资金进行现金管理存在空窗期的事项进行追认。保荐机构已敦促公司加强对募集资金的管理工作，完善相关内控措施，截至本报告出具日，公司已加强对募集资金管理及证券法律法规的学习，进一步完善募集资金使用的内部审批流程，完成相应整改。

除上述使用闲置募集资金进行现金管理存在授权空窗期未及时赎回的情形外，2024 年度，公司及子公司均严格按照《募集资金管理制度》的规定，存放和使用募集资金。

（五）募集资金专户存储情况

截至 2024 年 12 月 31 日，募集资金专户的余额如下：

公司名称	开户银行	银行帐号	余额（元）
亚信安全科技股份有限公司	招商银行股份有限公司南京鼓楼支行	125905906410555	3.18
亚信安全科技股份有限公司	中国工商银行股份有限公司北京长安支行	0200048519200863155	-
亚信安全科技股份有限公司	平安银行股份有限公司南京分行	15202201070177	2,364.77

公司名称	开户银行	银行帐号	余额（元）
亚信安全科技股份有限公司	南京银行股份有限公司南京分行	142290000002318	820.58
亚信科技（成都）有限公司	招商银行股份有限公司南京鼓楼支行	010900157010111	1,292,590.24
亚信科技（成都）有限公司	中国工商银行股份有限公司北京长安支行	0200048519200864181	285,894.39
亚信科技（成都）有限公司	南京银行股份有限公司南京分行	0187250000001743	4,089,161.39
南京亚信信息安全技术有限公司	南京银行股份有限公司南京分行	0187270000001742	6,029.63
募集资金账户余额			5,676,864.18
亚信安全科技股份有限公司	民生银行股份有限公司北京分行	633902478	27.54
亚信科技（成都）有限公司	民生银行股份有限公司北京分行	635590959	353,882.90
协定存款			353,910.44
募集资金专户余额			**6,030,774.62**
结构性存款			**50,000,000.00**
合计			**56,030,774.62**

十、控股股东、实际控制人、董事、监事和高级管理人员的持股、质押、冻结及减持情况

截至 2024 年 12 月 31 日，公司控股股东亚信信远（南京）企业管理有限公司及其一致行动人合计直接持有公司股票 190,902,237 股，合计持股比例为 47.72%;实际控制人田溯宁先生直接持股数量为 586,492 股，持股比例为 0.15%。公司董事、监事和高级管理人员未直接持有公司股票。公司控股股东及其一致行动人、实际控制人直接持有的公司股票未发生减持，也不存在质押、冻结等情形。

十一、上海证券交易所或保荐机构认为应当发表意见的其他事项

无。

（以下无正文）

（本页无正文，为《中国国际金融股份有限公司关于亚信安全科技股份有限公司2024年度持续督导跟踪报告》之签章页）

保荐代表人：

江　涛　　徐石晏

中国国际金融股份有限公司

2025 年 5 月 16 日