公司代码:603232 公司简称:格尔软件

格尔软件股份有限公司

2025 年度报告摘要

第一节 重要提示

1、本年度报告摘要来自年度报告全文,为全面了解本公司的经营成果、财务状况及未来发展规划,投资者应当到www.sse.com.cn网站仔细阅读年度报告全文。

2、本公司董事会及董事、高级管理人员保证年度报告内容的真实性、准确性、完整性,不存在虚假记载、误导性陈述或重大遗漏,并承担个别和连带的法律责任。

3、公司全体董事出席董事会会议。

4、上会会计师事务所(特殊普通合伙)为本公司出具了标准无保留意见的审计报告。

5、董事会决议通过的本报告期利润分配预案或公积金转增股本预案

经上会会计师事务所(特殊普通合伙)审计,公司2025年度实现归属于上市公司股东的净利润为-84,766,343.86元。根据《公司法》《公司章程》的有关规定,由于公司2025年经审计归属于上市公司股东的净利润为负数,未实现盈利,因此拟定2025年度不进行利润分配,也不进行资本公积转增股本。该预案尚需提交股东会审议。

截至报告期末,母公司存在未弥补亏损的相关情况及其对公司分红等事项的影响

□适用 √不适用

第二节 公司基本情况

1、公司简介

公司股票简况				
股票种类	股票上市交易所	股票简称	股票代码	变更前股票简称
A股	上海证券交易所	格尔软件	603232	无

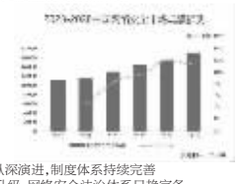
联系人和联系方式	董事会秘书	证券事务代表
姓名	孔令钢	吕昊轩
联系地址	上海市松江区泗泾镇沐川路58弄1-7号G60国用密码产业基地A2楼	上海市松江区泗泾镇沐川路58弄1-7号G60商用密码产业基地A2楼
电话	021-62327028	021-62327028
传真	021-62327015	021-62327015
电子信箱	stock@koal.com	stock@koal.com

2、报告期公司主要业务简介

2025年适逢《密码法》颁布实施五周年,亦是“十四五”规划全面收官之年,我国网络与数据安全行业呈现“制度深化、技术跃迁、场景落地”的阶段性特征。这一年,密码技术的角色定位发生深刻转变——从过去满足等级保护、密评要求的合规工具,跃升为支撑新质生产力发展的核心安全底座。密码不再只是系统补丁式的安全配件,而是贯穿数据要素流通全流程、算力基础设施、智能体安全交互的信任基础设施,成为护航数字中国建设的底层基石。

技术端,行业正面临“经典密码向抗量子密码迁移”与“人工智能安全治理制度化”的双重拐点。一方面,抗量子密码标准体系加速构建,商用密码产业正式从“实验探索”迈入“合规准备”阶段;另一方面,生成式人工智能的广泛应用推动AI安全治理从伦理倡议走向制度落地,密码技术在保障AI系统可信运行中的核心地位日益凸显。市场端,在数字中国战略深入推进、数据安全法规体系持续完善以及新技术应用加速落地的多重驱动下,行业增长整体增长的基本面依然稳健,根据IDC预测,中国网络安全市场规模将从2023年的110亿美元增长至2028年的171亿美元,年复合增长率达9.2%。

然而在总量稳健增长的背后,市场正呈现增量机遇与存量压力并存的双重格局:一方面,数据要素×三年行动进入攻坚阶段,可信数据空间、低空经济、智能物联等新场景加速落地,为商用密码创造了增量空间;另一方面,受宏观经济环境影响,关键信息基础设施行业的客户预算普遍承压,行业竞争从政策红利驱动转向能力深耕驱动,短期业绩面临一定调整压力。展望未来,随着数字中国建设的持续推进、数据安全法规的全面落地以及抗量子密码等前沿技术的产业化提速,商用密码行业有望在政策驱动与需求回暖的双重作用下,迈入高质量发展的新阶段。



(一)政策法规纵深演进,制度体系持续完善

1.基础法律修订升级,网络安全法治体系日趋完备

2025年是我国网络安全基础法律修订的关键之年,我国网络安全法治体系由此迈入全新发展阶段。2025年10月,第十四届全国人民代表大会常务委员会第十八次会议表决通过《关于修改〈中华人民共和国网络安全法〉的决定》,完成这部法律自2017年施行以来的首次重大修订。本次修订新增人工智能安全监管、数据跨境流动等关键条款,全面升级法律责任体系,显著加大对网络运营者未履行安全保护义务的处罚幅度,对关键信息基础设施运营者不履行法律规定义务的情形进一步加大处罚力度。同期,《治安管理处罚法》完成修订,增列非法获取计算机信息系统数据、非法控制计算机信息系统等违法行为,进一步补齐了网络安全违法行为的法律追责制度短板。

2.数据治理纵深推进,要素市场化制度全面落地

数据要素市场化配置改革进入深水区,数据安全治理与数据流通利用双轮驱动,并重发展制度格局基本成型。数据安全层面,全生命周期监管体系持续完善。2025年1月1日起,《网络数据安全管理条例》全面实施,与《数据安全法》《个人信息保护法》形成“三位一体”监管体系,聚焦网络数据分类分级、跨境流动、安全防护等核心环节,构建了覆盖数据处理全生命周期的监管框架。2025年8月,国务院公布《政务数据共享条例》,衔接上位监管要求,针对政务数据安全共享提出补充性、创新性规定,填补了我国在政务数据共享领域的立法空白。数据流动利用层面,要素市场化全链条规则体系全面搭建。围绕在公共数据资源开发利用,国家发展改革委和国家数据局陆续发布《公共数据资源授权运营实施规范(试行)》《公共数据资源登记管理暂行办法》《关于建立公共数据资源授权运营价格形成机制的通知》,形成覆盖公共数据授权运营、登记确权、价格管理的全链条制度闭环,为数据要素市场化流通、合规化交易奠定了制度基础。

3.关基保护规则细化,商用密码使用管理强化

关键信息基础设施安全保护制度持续完善,商用密码使用管理要求进一步细化和强化。在国家级顶层规则层面,2025年6月,国家密码管理局、国家互联网信息办公室、公安部联合发布《关键信息基础设施商用密码使用管理规定》,明确关键信息基础设施运营者的商用密码使用责任,细化商用密码使用的具体要求,建立监督检查及法律责任机制。该规定在《密码法》《商用密码管理条例》《关键信息基础设施安全保护条例》基础上,对关键信息基础设施商用密码使用管理要求进行进一步细化,强化了运营者的主体责任,明确了商用密码使用的具体要求,并要求定期开展商用密码应用安全性评估。在行业层面,国家邮政局发布《邮政业关键信息基础设施安全保护管理办法(试行)》,国家能源局发布《能源行业数据安全管理办法(试行)》,各行业关基保护规则持续细化。在监管层面,公安机关部署“护网-2025”专项行动,全力保护网络安全,加强关键信息基础设施保护、重要系统安全检测。

4.AI治理框架确立,新技术安全规制提速

人工智能安全治理从伦理宣示走向制度化落地,《网络安全法》首次在基础法律层面确立人工智能治理顶层设计。《网络安全法》新增第二十条,明确提出“国家支持人工智能技术研发和应用,推动人工智能安全评估和监管制度建设”,确立“支持研发”与“加强监管”的总基调,为后续制定人工智能伦理规范、安全评估等细则提供了上位法依据。国家互联网应急中心牵头组织联合制定发布《人工智能安全治理框架2.0版》,结合人工智能技术发展和应用实践,持续跟踪风险变化,完善优化风险分类,研究探索风险分级。GB/T 45652-2025《网络安全技术生成式人工智能预训练和优化训练数据安全规范》等国家标准相继发布,为人工智能应用提供安全合规指引。

5.行业政策精准施策,重点领域合规要求提升

政务、金融、能源、医疗等重点行业数据安全政策密集出台,行业合规要求持续提升。在金融领域,中国人民银行发布《中国人民银行业务领域数据安全管理办法》,中国人民银行、中国证监会联合发布《金融基础设施监管管理办法》,对金融基础设施运营机构技术系统及管理机制提出明确要求,强化数据安全的商用密码保护。在政务领域,《政务数据共享条例》《公共安全视频图像信息系统管理条例》相继出台,国务院发布《电子印章管理办法》,规范电子印章管理。在能源领域,《能源行业数据安全管理办法(试行)》明确能源行业重要数据的处理者在数据全生命周期各环节应综合运用加密、鉴权、认证、脱敏、校验、审计等技术手段进行安全保护。在医疗领域,《医药工业数智化转型实施方案(2025—2030年)》推动落实数据管理能力成熟度、个人信息保护等评估。重点行业政策的密集出台,进一步提升了各领域对密码技术应用的合规需求。

(二)抗量子密码研究推进,安全底座前瞻布局

量子计算技术的快速发展对传统密码体系构成系统性安全威胁,全球抗量子密码(PQC)研究和布局全面提速。美国国家标准与技术研究院(NIST)于2024年8月正式发布了全球首批3个抗量子加密标准,标志着抗量子密码从“实验探索”阶段进入“合规准备”阶段。我国高度重视抗量子密码研究,国家级重点研发计划中设立了“抗量子计算密码”项目,科技部、工信部等部门也设立了多个抗量子密码相关的科研项目。2025年2月,商用密码标准研究院宣布开启面向全球的新一代密码算法征集活动,我国抗量子密码的标准制定工作正式启动,为全生态构建奠定了技术基础。

国内商用密码厂商在抗量子算法工程实现及产业化方面取得积极进展,抗量子密码产品在政务、军工、金融等核心领域率先开展试点。国内头部企业已完成部分密码产品的抗量子能力升级,实现了NIST抗量子算法及中国抗量子算法的工程化,相关产品在通过权威机构验证后,已在银行、证券等行业开展应用试点,为抗量子密码迁移积累了实践经验。

全球主要国家正设定抗量子密码迁移最终节点,优先开展高风险系统的迁移准备工作。各国政府和企业认识到,量子计算机的发展将威胁现有密码系统的安全性,关键信息基础设施、金融系统、政府通信等高价值目标需要优先进行抗量子密码迁移。密码治理规则持续细化,从“实验探索”转向“合规准备”,抗量子密码迁移已成为全球网络安全领域的共识和紧迫任务。随着抗量子密码标准的逐步完善和产业生态的持续发展,密码安全底座正在经历从传统密码向抗量子密码的代际更迭,为数字经济的长期安全发展奠定基础。

(三)人工智能深度融合,安全范式智能重构

生成式人工智能(LLM)的爆发式应用重构了网络空间的风险结构,AI安全治理从伦理宣示走向制度化落地。《网络安全法》新增第二十条,首次在基础法律层面确立人工智能治理顶层设计,明确提出“国家支持人工智能技术研发和应用,推动人工智能安全评估和监管制度建设”,确立“支持研发”与“加强监管”的总基调。国家互联网应急中心牵头组织联合制定发布《人工智能安全治理框架2.0版》,结合人工智能技术发展和应用实践,持续跟踪风险变化,完善优化风险分类,研究探索风险分级。GB/T 45652-2025《网络安全技术生成式人工智能预训练和优化训练数据安全规范》等国家标准相继发布,为人工智能应用提供安全合规指引。

人工智能大模型的训练和应用催生了全新的数据安全需求,密码技术与AI安全深度融合。大模型训练涉及海量敏感数据,需要通过联邦学习框架,结合同态加密、多方安全计算、差分隐私等密码技术,,在确保训练数据隐私安全的前提下打通多方协作壁垒,推动AI技术在医疗、金融等敏感行业的深度应用。AI智能体(AI Agent)的快速发展对身份认证和安全防护提出了新的要求,各类设备、应用、智能体需要构建高效、智能的身份安全防护体系,机器身份管理成为密码技术应用的新方向。

AI技术亦反哺密码领域,机器学习算法可优化密码系统的攻击检测效率,辅助提升密钥管理全生命周期的运维与风险预警能力,形成“安全-智能”双向赋能生态。人工智能技术应用于密码分析、密钥管理、威胁检测等领域,提升了密码系统的智能化水平。智能防御能力不断提升,密码与AI的融合成为网络安全领域的重要发展趋势。人工智能的“自主性”与“技术不可知性”突破了传统法律可控性前提,网络空间治理正向“智能增强型安全范式”整体演进。在这一背景下,密码技术作为保障AI系统安全的基础性技术,将在AI安全治理中发挥越来越重要的作用。

(四)数据要素流通提速,安全基础设施升级

数据要素市场化配置改革不断深化,数据要素流通基础设施加速构建。《“数据要素×”三年行动计划(2024—2026年)》推动数据要素市场化进程全面提速,国家数据局数据显示,2024年全国数据市场交易规模预计超1,600亿元,同比增长30%以上,其中场内市场数据交易(含备案交易)规模预计超300亿元,同比实现翻番。公共数据资源利用制度体系不断完善,国家发展改革委和国家数据局发布《公共数据资源授权运营实施规范(试行)》《公共数据资源登记管理暂行办法》