鹏鼎控股（深圳）股份有限公司

2025 年度新兴风险执行情形(更新日期: 2026年3月)

为达成企业永续发展的目标，分析公司在营运过程中可能面临的冲击和挑战，持续关注国际政经情势变化对企业的威胁，以及错误信息与造假信息带来的风险。根据2026年1月14日世界经济论坛发布的《全球风险报告》，在近两年的十大新兴风险中，国际政经情势的变化对企业永续发展构成了严重威胁，涵盖了国际武装冲突、社会两极化、不平等与非自愿迁徙等议题。此外，错误信息与造假信息的风险也不容忽视，其定义为持续存在的假讯息（无论是故意还是无意）的广泛传播，对公众舆论产生巨大影响，导致对事实和权威的不信任，涉及伪造、冒名顶替和操纵等内容。这些风险提醒我们在变幻莫测的全球局势中，应更加谨慎地应对各种挑战。

1. 国际政经情势变化对公司的威胁

风险描述	对公司潜在影响	控制执行计划	执行情形
依据《全球风险报告》，全球贸易格局面临结构性调整，联合国预测 2026 年全球贸易增速将放缓至 2.2%，美国关税政策不确定性持续对全球供应链造成冲击，有效关税税率居高不下导致跨国贸易成本显着上升。 多边主义退潮趋势明显，68%受访者预计未来十年全球呈现多极化或碎片化秩序，区域贸易壁垒、投资法规变动频率加快，进一步加剧市场不确定性。 在高科技领域，半导体、人工智能等核心产业的技术管制范围持续扩大，不仅涵盖终端产品，更延伸至关键材料、制程设备及算法领域，对科技制造业的全球布局与技术迭代构成持续压力。 此类风险相互迭加，导致全球供应链韧性面临严峻考验，也使公司在跨区域营运、投资规划及资源分配上面临更高的决策难度。	国际政经情势对公司营运全链条的影响，主要体现在四大维度： 供应链韧性压力升级： • 因保护主义政策导致关税成本增加、通关流程复杂化。 • 区域贸易协议导致的供应链重构带来额外的迁移成本。 市场拓展与盈利空间受限： • 全球贸易增速放缓导致终端市场需求收缩，迭加全球最低税赋制的全面落地，公司海外市场市占率提升面临阻力，净利润率受挤压。 投资与筹资风险加剧： • 多极化格局下，导致海外投资项目面临更高的政策不确定性。 • 汇率波动、国际融资成本上升，进一步加大资金调度难度，财务结构面临考验。 技术研发与产业升级受阻： • 高科技领域的技术管制导致核心技术授权、关键设备采购受限。 • 全球技术标准碎片化趋势，产业升级面临调整压力。	**1. 内部韧性建设：** • 供应链多元化布局以降低保护主义之冲击、减少进出口成本，并提高供货稳定度。 • 强化财务风险管控，并分散投资以降低汇率及投资风险，运用财务工具避险。 • 优化全球产能配置，提升产能利用率与市场响应速度。 • 定期召开审计暨风险委员会议审视国际局势变化，并即早调整和研拟因应对策。 **2. 外部生态共建：** • 透过与各方利害关系人之合作，更快了解国际政经局势之变化，使公司策略更符合现况。 • 深化与核心客户、供货商的战略合作，共建抗风险供应链联盟，共享政策信息、联合开发替代方案，提升产业链整体韧性。	**1. 内部韧性建设：** • 增加产学研合作，提升自身竞争力，2025年共与23所院校进行产学研发项目合作院校。 • 技术自主研发投入增加，2025年新增专利获证194件，较2024年提升13.3%。 • 供应链筛选100%依循 “Second Source 原则”，避免单一来源及供货商断链。 • 2025年共召开经营委员会23次和资本支出审议会30次，定期检视资本资出避免过度投资。 • 全球产能布局进一步优化，泰国生产基地完成二期扩建并投产。 • 以「维新使命，数智为纲」深化数位转型，母公司成立数转创新加速器，推动跨部门合作与创新思维，以培育新世代人才和接班团队。 **2. 外部生态共建：** • 积极获取政经形势分析报告，参与国际政经局势研讨会与在地行业协会圆桌会，以交流见解。 • 与当地高校产学联盟，以为人力资源。

2. 错误信息与造假信息

风险描述	对公司潜在影响	控制执行计划	执行情形
随着生成式人工智能技术的规模化应用，错误信息与造假信息风险已跃升为全球短期核心技术风险，其传播速度、影响范围与识别难度均呈指数级增长。 大模型技术能够生成高真实感的文本、图像、音视频等多模态内容，普通公众不借助专业工具已难以辨识真伪，且生成速度快、成本低，导致造假场景日益多样化，包括 AI 换脸诈骗、虚假产品缺陷视频、伪造财务数据等违规违法事件频发。 此类风险的爆发具有突发性与传染性，若应对不及时，可能快速引发市场恐慌与利害关系人信任危机。	错误信息与造假信息对公司的潜在影响主要体现在四大层面： 品牌声誉与市场信任受损： • AI 生成的虚假信息在网络快速传播，可能引发消费者、投资者恐慌，导致股价波动；若应对不及时，可能造成长期品牌信誉损失。 营运效率与决策质量下降： • 供应链中的虚假需求数据可能导致生产计划失误，出现产能过剩或短缺。 • 内部市场分析报告可能误导经营决策，造成市场布局失误。 数据安全与生产安全风险： • 工业控制系统中的虚假数据可能引发产品质量问题甚至生产安全事故。 • 员工因点击 AI 生成的钓鱼邮件，可能导致内部机密数据泄露。 合规成本与法律风险增加： • 相关法规要求企业对自身发布的内容及员工行为承担相应责任，若因管理不当导致未履行标识义务或传播造假信息，可能面临行政处罚。	**1. 内部强化管控：** • 强化员工信息安全与鉴伪能力培训，将 AI 造假识别、钓鱼信件防范等内容纳入资安教育训练，定期开展演练，提升员工对高仿真造假信息的识别与应对能力。 • 藉由防垃圾邮件机制，过滤可疑信件以避免员工点开其信件，造成信息外泄。 • 严格管控电子设备与网络使用，降低数据与数据外泄的可能。 • **2. 外部协同联动：** • 由发言人单位成立应变小组以实时因应错误或造假信息，达到防止恶化之目的。 • 法务单位提前做好相关诉讼之准备，以降低造假信息造成的损失及影响。 • 藉由倡导诚信经营之理念，提升利害关系人对消息的判断力。 • 建立良好之信誉与口碑，以预防及降低公司受错误信息之冲击。	**1. 内部强化管控：** • 每月召开资安会议进行资安意识倡导。 • 2025年资安教育训练课程累计69,910小时、参与课程总计352,850人次。 • 为防范网络攻击与搜集网络态势，平均每月阻挡超过10,817件网络攻击及71,779封恶意邮件，防止恶意行为造成公司损失。 • 公司已导入舆情监测系统，系统自动检测并收集公司及子公司不实消息，再由工作人员进行处理。 • 严格管控员工办公设备，未经授权不得安装使用标准配置以外软件，并于员工手册中订定奖惩制度，提升员工资安意识。 • 本公司 2025年未收到主管机关通报之错误或造假信息之事件。 **2. 外部协同联动：** • 积极维护公司官网，全面且及时发布新闻与信息披露，提升公众及利害关系人对官方信息的信任度与造假信息的辨识力。 • 成立品牌策略处统整公司社群媒体账号，并建立社群媒体信息发布审核机制，确保对外发布信息真实性及一致性。 • 软硬件异地备援，每年进行2次消灾与备份还原演练，以为因应。 • 不定期（每年至少一次）举办倡导诚信经营理念课程供利害关系人参与。

Avary Holding (Shenzhen) Co., Limited

2025 Implementation Result of Emerging Risks (Updated: March 2026)

To achieve the goal of sustainable development, the company analyze the potential impacts and challenges it may face during the transformation process, and continuously formulate strategies to address the challenges of sustainable operations. According to the "Global Risks Report" released by the World Economic Forum on January 14, 2026, shifts in the international political and economic situation pose a severe threat to corporate sustainability among the top ten emerging risks of the past two years, covering issues such as interstate armed conflict, societal polarization, inequality, and involuntary migration. Furthermore, the risk of "misinformation and disinformation" cannot be ignored. It is defined as the widespread circulation of persistent false information (whether intentional or unintentional), which exerts a significant influence on public opinion, leading to a distrust of facts and authority, and involves forgery, impersonation, and manipulation. These risks serve as a reminder for us to navigate various challenges with greater prudence amidst an unpredictable global environment.

1. Threat of international political and economic situation changes to the company

Description of risk	Potential impact on the Company	Control the implementation plan	Implementation status
According to the "Global Risks Report," the global trade landscape is undergoing structural adjustments. The United Nations projects that global trade growth will slow to 2.2% in 2026. Ongoing uncertainty in U.S. tariff policies continues to impact global supply chains, while persistently high effective tariff rates have led to a significant rise in cross-border trade costs. The retreat of multilateralism is becoming increasingly evident, with 68% of respondents expecting a multipolar or fragmented global order over the next decade. The accelerating frequency of changes in regional trade barriers and investment regulations is further exacerbating market uncertainty.	The impact of the international political and economic situation on the company's entire operational chain is primarily reflected across four major dimensions: <u>Escalating Pressure on Supply Chain Resilience:</u> • Increased tariff costs and more complex customs clearance processes resulting from protectionist policies. • Additional migration costs arising from supply chain restructuring driven by regional trade agreements. <u>Constraints on Market Expansion and Profitability:</u> • Shrinking end-market demand due to the global trade slowdown, coupled with the full implementation of the Global Minimum Tax (GMT), creates headwinds for increasing the	**1. Building internal resilience:** • Diversify supply chain layout to mitigate the impact of protectionism, reduce import-export costs, and enhance supply stability. • Strengthen financial risk management and diversify investments to lower foreign exchange and investment risks, utilizing financial instruments for hedging. • Optimize global capacity allocation to improve capacity utilization and market responsiveness. • Convene regular Audit and Risk Committee meetings to review shifts in the international landscape, enabling early adjustment and the formulation of response strategies. **2. External Ecosystem Co-construction:** • Collaborate with various stakeholders to gain faster insights into changes in the	1**. Building internal resilience:** • Expanded Industry-Academia-Research collaboration to enhance core competitiveness. In 2025, the company collaborated with 23 academic institutions on joint R&D projects. • Increased investment in independent R&D, with 194 new patents granted in 2025, representing a 13.3% increase compared to 2024. • 100% adherence to the "Second Source Principle" in supply chain screening to avoid single-source dependency and supply chain disruptions. • Convened 23 Management Committee meetings and 30 CAPEX Review Committee meetings in 2025 to regularly review capital expenditures and prevent over-investment. • Further optimized global capacity layout, with the completion and commencement of production for Phase II of the Thailand manufacturing base.

Description of risk	Potential impact on the Company	Control the implementation plan	Implementation status
In high-tech sectors, the scope of technology controls in core industries—such as semiconductors and artificial intelligence—continues to expand. These controls now extend beyond end products to encompass critical materials, manufacturing equipment, and algorithms, placing sustained pressure on the global footprint and technological iteration of the tech manufacturing industry. The overlapping of these risks poses a severe test for global supply chain resilience, significantly increasing the complexity of decision-making for the company in terms of cross-regional operations, investment planning, and resource allocation.	Heightened Risks in Investment and Financing: • In a multipolar landscape, overseas investment projects face higher policy uncertainty. • Exchange rate volatility and rising international financing costs further increase the difficulty of capital deployment, placing the company's financial structure under significant strain. Obstructions to Technological R&D and Industrial Upgrading: • Technology controls in high-tech sectors lead to restrictions on core technology licensing and the procurement of critical equipment. • The trend toward fragmentation of global technical standards exerts pressure on the pace of industrial upgrading and necessary adjustments.	international political and economic environment, ensuring corporate strategies remain aligned with current realities. • Deepen strategic partnerships with core customers and suppliers to build anti-risk supply chain alliances, sharing policy information and co-developing alternative solutions to enhance the overall resilience of the industrial chain.	• Deepened digital transformation under the mission of " Innovation-Driven, Digitally-Led", the parent company has established a digital transformation innovation accelerator to promote cross-departmental collaboration and innovative thinking in order to cultivate a new generation of talents and succession teams. • **2. External Ecosystem Co-construction:** • Actively acquire political and economic analysis reports and participate in international geo-political forums as well as local industry association roundtables to exchange strategic insights. • Establish industry-academia alliances with local universities to secure and cultivate a robust pipeline of human resources.

2. Misinformation and disinformation

Description of risk	Potential impact on the Company	Control the implementation plan	Implementation status
With the large-scale application of Generative AI (GenAI) technologies, the risks of misinformation and disinformation have surged to become a core global short-term technical risk. Their speed of dissemination, scope of impact, and difficulty of detection are all increasing exponentially. Large Language Model (LLM) technologies can generate highly realistic multimodal content, including text,	The potential impact of misinformation and disinformation on the company is primarily reflected across four major levels: Damage to Brand Reputation and Market Trust: • AI-generated false information spreading rapidly online can trigger panic among consumers and investors, leading to stock price volatility. Failure to respond	**1. Strengthen internal control:** • Strengthen employee training in information security and authentication. Incorporate AI forgery detection and phishing prevention into security education programs, and conduct regular drills to enhance employees' ability to identify and respond to hyper-realistic fake information. • Leverage anti-spam mechanisms to filter suspicious emails, preventing information leakage caused by employees	**1. Strengthen internal control:** • Conduct monthly information security meetings to promote security awareness across the organization. • Accumulated 69,910 hours of information security training in 2025, with a total of 352,850 participants. • To defend against cyberattacks and monitor network security posture, the company blocked an average of over 10,817 cyberattacks and 71,779 malicious emails per month, successfully preventing losses from malicious activities.

images, audio, and video, making it nearly impossible for the general public to distinguish truth from falsehood without professional tools. Furthermore, the high speed and low cost of generation have led to increasingly diverse fraudulent scenarios, such as AI face-swapping scams, fake product defect videos, and forged financial data. The eruption of such risks is often sudden and contagious. If not addressed promptly, they can rapidly trigger market panic and a crisis of trust among stakeholders.	promptly may result in long-term loss of brand credibility. <u>Decline in Operational Efficiency and Decision Quality:</u> • False demand data within the supply chain may lead to production planning errors, resulting in either capacity surplus or shortages. • Inaccurate internal market analysis reports may mislead management decisions, leading to strategic missteps in market positioning. <u>Data Security and Operational Safety Risks:</u> • False data injected into Industrial Control Systems (ICS) could trigger product quality issues or even lead to industrial safety accidents. • Employees clicking on AI-generated phishing emails may lead to the leakage of internal confidential data. <u>Increased Compliance Costs and Legal Risks:</u> • Relevant regulations require enterprises to assume responsibility for self-published content and employee conduct. If mismanagement leads to a failure in fulfilling labeling obligations or results in the dissemination of fabricated information, the company may face administrative penalties.	inadvertently opening malicious links or attachments. • Strictly control electronic device and network usage to minimize the risk of data and information breaches. **2. External collaboration:** • The Spokesperson's Office shall establish a response task force to provide real-time countermeasures against misinformation or disinformation, ensuring timely containment and preventing further escalation. • The Legal Department shall proactively prepare for litigation to mitigate losses and impacts caused by fabricated information. • Promote the philosophy of business integrity to enhance stakeholders' critical judgment regarding external news and information. • Build a strong corporate reputation and brand equity as a proactive measure to prevent and buffer the impact of misinformation on the company.	• Implemented a public opinion monitoring system that automatically detects and collects misinformation regarding the company and its subsidiaries, which is then processed by designated personnel. • Strictly control employee office equipment, prohibiting the installation of unauthorized software beyond the standard configuration. A system of rewards and penalties has been established in the Employee Handbook to further enhance security awareness. • Zero incidents of misinformation or disinformation were reported by regulatory authorities to the company in 2025. **2. External collaboration:** • Actively maintain the official corporate website to ensure comprehensive and timely news and information disclosure, enhancing trust among the public and stakeholders in official information and their ability to identify fake information. • Establish the Brand Strategy Department to consolidate the company's social media accounts and implement a content review mechanism, ensuring the authenticity and consistency of all externally released information. • Implement off-site backup for both hardware and software, conducting two disaster recovery and backup restoration drills annually to ensure operational continuity. • Organize business integrity philosophy training sessions periodically (at least once a year) for stakeholders to participate in.