
上海汉得信息技术股份有限公司

公司风险管理制度

(2026 修订)

发布日期： 二〇二六年一月

实施日期： 二〇二六年一月

第一章 总则

第一条 目的与依据

为建立系统化、结构化的风险管理程序，有效识别、评估、监控及应对公司面临的重大内外部风险，保障公司战略目标的实现、资产安全及运营的可持续性，特制定本制度。

第二条 适用范围

本制度适用于本公司及其所有控股子公司（以下简称公司）的所有业务活动、职能部门及管理流程。

第三条 核心目标

- （一）建立正式的书面程序，确保重大风险能被及时、系统地辨认。
- （二）对已识别的风险进行合理评估，确定其发生的可能性及潜在影响。
- （三）根据评估结果，制定并执行有效的风险管理（包括规避、降低、转移或接受）策略。
- （四）将风险管理嵌入公司战略决策与日常运营，形成常态化的风险管理文化。

第二章 风险管理组织与职责

第四条 董事会对公司风险管理体系的有效性承担最终责任，负责审批本制度及重大风险管理政策，并监督其执行。

第五条 审计委员会在董事会授权下，负责监督本制度的执行情况，审阅重大风险评估结果及年度风险管理报告。

第六条 管理层为风险管理的执行领导层，负责：

- （一）建立并维护有效的风险管理框架和流程。
- （二）确保资源投入，推动风险管理文化。
- （三）审批《年度风险评估结果》及《重大风险管理计划》。
- （四）向董事会及审计委员会报告重大风险状况。

第七条 运营管理部作为制度的主导执行部门，是公司的风险管理部门，负责：

- （一）组织、协调年度风险识别与评估工作。
- （二）维护《公司重大风险登记册》。
- （三）跟踪《风险管理行动计划》的执行。
- （四）编制年度《风险管理报告》。

第八条 各职能部门及交付部门作为风险管理的第一道防线，负责：

- （一）持续识别、评估并管理其职责范围内的风险。
- （二）向风险管理部门提供准确、及时的风险信息。
- （三）执行经批准的风险应对措施。

第三章 风险管理核心流程

第九条 风险辨认

（一）识别范围：应全面覆盖内外部环境，包括但不限于：

- 1、战略风险：市场竞争、技术颠覆、并购整合、战略伙伴关系等。
- 2、运营风险：软件服务行业聚焦：核心人才流失、项目交付失败/延期、关键供应商中断、服务质量（SLA）不达标、业务连续性（如数据中心故障）、知识产权侵权等。
- 3、财务风险：现金流中断、应收账款坏账、成本超支、汇率利率波动等。
- 4、合规风险：数据隐私与保护（如 GDPR、PIPL）、网络安全法规、软件许可合规、劳动法规等。

5、技术风险：网络安全攻击、数据泄露、核心技术落后、系统架构重大缺陷等。

（二）识别方法：每年至少组织一次由管理层及各部门负责人参与的正式风险识别会议。同时，结合行业分析、审计发现、客户投诉、项目复盘等多渠道信息进行日常识别。

第十条 风险评估

（一）评估标准：采用“财务影响可能性”与“运营/战略影响程度”二维矩阵进行评估。公司制定如下量化或定性标准及风险评价矩阵图：

程度标准	财务影响可能性	运营/战略影响程度
重大	损失 > 年收入 5%	导致战略目标无法达成，或关键业务长期中断。
高	损失=年收入 1%-5%	对战略目标造成重大延误，或业务严重中断。
中	损失=年收入 0.5%-1%	对部分业务造成显著影响，需要管理层介入。
低	损失 < 年收入 0.5%	影响轻微，可由部门内部解决，并保留处理记录。

风险评价矩阵图

财务 影响可能性 运营/战略 影响程度	影响轻微	显著影响	重大延误或业务严重中断	战略目标无法达成或关键业务长期中断
损失 > 年收入 5%	中*/高*	高	极高	极高
损失=年收入 1%-5%	低*/中*	中	高	极高
损失=年收入 0.5%-1%	低	低	中	高
损失 < 年收入 0.5%	低	低	低*/中*	中*/高*

*考虑实际情况的影响程度对事件进行判断。

（二）重大风险及响应措施：根据评估结果，在风险评价矩阵中位于高、极高区域的风险，应被定义为‘重大风险’，纳入《公司重大风险登记册》进行重点管理，并立即汇报相关风险至公司管理层，如风险事件涉及的公告及披露，应汇报审计委员会及董事会。

（三）一般风险及响应措施：根据评估结果，在风险评价矩阵中位于中区域的风险，应被定义为“一般风险”，应立即汇报相关风险涉及部门负责人及风险管理部门，风险管理部门对其进行登记并持续监督，记录处理结果，并反馈于《风险管理报告》中汇报至管理层。如风险事件涉及重大业务/财务影响，还应立即汇报总经理。

（四）低风险及响应措施：根据评估结果，在风险评价矩阵中位于低区域的风险，应被定义为“低风险”，应立即汇报风险管理部门进行登记，风险管理部门对处理结果进行记录，并反馈于《风险管理报告》中汇报至管理层。

第十一条 风险管理

（一）针对每一项“重大风险”，责任部门须制定并选择一项或组合多项应对策略：

- 1、风险规避：停止或退出可能导致风险的活动。
- 2、风险降低：采取内部控制措施降低可能性或影响。
- 3、风险转移：通过保险、外包或合同条款将风险转移给第三方。
- 4、风险接受：在风险偏好内，主动承担该风险，并准备应急计划。

风险管理部门汇总编制《重大风险管理计划》，并提交管理层审批。

（二）针对“一般风险”和“低风险”，应形成风险应对策略，风险管理部门汇总《风险管理行动计划》，明确责任部门、负责人、关键里程碑、所需资源及完成时限。

第十二条 风险监控与报告

（一）动态监控：风险责任部门需持续监控风险状态及应对措施的执行效果，风险管理部门进行跟踪，记录风险变化。

（二）定期报告：

年度报告：风险管理部门编制年度《风险管理报告》，内容应包括：本年度风险评估回顾、重大风险变化分析、风险管理有效性总结、下年度风险管理工作重点。该报告经管理层审核后，提交审计委员会及董事会审阅。

第四章 与内部控制体系的衔接

第十三条 风险管理是内部控制的基础。本制度识别出的重大风险，特别是需要通过“降低”策略管理的运营与合规风险，必须作为公司内部控制体系设计与优化的重要输入。相关控制活动应体现在各业务制度中。

第十四条 内部审计部门在开展审计工作时，应参考《公司重大风险登记册》，将重大风险领域作为审计重点，评估相关控制措施的有效性。

第五章 附则

第十五条 制度审查

本制度至少每两年由风险管理部门牵头复审一次，或在公司业务、组织架构及外部环境发生重大变化时及时修订。

第十六条 解释权

本制度由公司风险管理部门负责解释。

第十七条 生效

本制度经董事会批准后生效。