# 第六章 用户需求

### 一、项目背景及情况

在数字化时代，信息已成为企业的核心资产之一，信息安全和业务连续性对于企业的稳定运营和可持续发展至关重要。随着信息技术在金融领域的广泛应用，公司的个人业务不断拓展，业务对信息系统的依赖程度日益加深。与此同时，信息安全威胁也呈现出多样化、复杂化的趋势，《网络安全法》《数据安全法》等一系列法律法规的出台，对企业在信息安全管理方面提出了明确的要求和严格的约束。鉴于公司信息科技专业人才资源有限、技术工具平台支持有待提升，为有效检查公司信息安全方面可能存在的问题，并结合业务发展及监管需要，有必要对公司信息安全管理情况进行审计。同时，按照《商业银行业务连续性监管指引》（银监发〔2011〕第104号）第十七条，“商业银行内部审计部门应当负责并定期开展全行业务连续性管理审计工作”；以及公司《业务连续性管理办法》（国金租发〔2020〕28号）第十四条，“审计部负责每三年对公司业务连续性管理情况开展一次全面审计”。

为加强公司信息安全管理，保障业务连续性，同时满足监管制度要求，根据经审批的2025年内部审计计划，公司审计部计划对公司信息安全管理情况和业务连续性管理情况开展审计。为保障审计质量，本次审计拟通过专项审计工作外包的方式，聘请第三方专业机构协助开展。

### 二、项目内容及相关要求

**（一）工作目标**

一是全面评估公司信息安全管理现状。通过审计，全面了解公司信息安全管理制度的建立健全情况、执行情况及存在的问题，提出针对性的改进建议。

二是检查业务连续性管理情况。依据《商业银行业务连续性监管指引》及公司《业务连续性管理办法》要求，对公司业务连续性管理的组织架构、策略制定、资源保障、演练实施等方面进行审计，确保业务连续性管理得到有效实施。

三是提升信息安全与业务连续性管理水平。通过审计发现的问题及改进建议，推动公司信息安全管理和业务连续性管理水平的提升，增强公司应对突发事件的能力。

**（二）工作内容**

1.信息安全管理审计

（1）制度建设审查：全面梳理公司现有的信息安全管理制度，检查其是否涵盖网络安全、移动安全、终端安全、数据安全、开发安全等各个方面，评估制度内容是否符合国家相关法律法规以及行业标准，是否随着公司业务发展和技术变化及时更新完善。

（2）执行情况检查：查看并验证各项信息安全管理制度在日常工作中的执行情况，例如网络访问控制策略是否严格执行，员工对终端安全管理规定的遵守程度，数据加密措施在数据存储和传输过程中的落实情况等，通过访谈、问卷调查、技术检测等多种方式收集证据，评估执行效果，并重点关注数据安全审批流程的执行情况。

（3）安全风险评估：利用专业技术工具和方法，对公司的信息系统进行安全漏洞扫描、渗透测试等，识别潜在的安全风险点，分析风险发生的可能性和影响程度，形成详细的风险评估报告，并提出针对性的风险应对建议。

2.业务连续性管理审计

（1）计划文档审查：审查公司业务连续性计划文档，检查其是否明确了关键业务及其恢复目标、恢复时间点，是否涵盖了各类可能的突发事件场景，如自然灾害、技术故障、人为破坏等，评估计划内容的合理性和完整性。

（2）应急演练评估：检查公司过去开展的业务连续性应急演练记录，评估演练的组织实施情况、演练效果，包括演练是否覆盖了所有关键业务环节，演练过程中发现的问题及改进措施的落实情况等。

（3）资源保障审查：审查公司为保障业务连续性所配备的资源，如备用数据中心、应急通信设备、关键岗位人员备份等，评估资源的充足性、可用性以及与业务连续性计划的匹配程度。

1. **工作要求**

\*1.服务商应组建由至少4人组成的审计团队，拟派出的审计团队成员（不含驻场负责人）中至少应有3人具有3年（含）以上IT审计工作经验，驻场负责人应具有8年（含）以上IT审计工作经验。审计团队成员应与应标时保持一致，不得擅自更换，团队主要负责人一经确定不得变更。

2.审计组应按格式起草审计方案，内容包括审计目的、审计依据、审计范围、审计内容要点、审计方法、实施步骤和时间安排、审计组成员及分工，审计部负责对审计方案进行复核及报批。

3.审计组应按经批准的审计方案实施审计，不得擅自扩大审计范围或减少审计事项，如确需扩展审计范围，应在报审计部审核并经公司审批同意后实施。审计组应对审计过程进行记录，撰写相应的工作底稿。工作底稿应包含审计发现、审计结论、定性依据、重要问题成因分析、审计意见及建议等内容。

4.审计组应进行现场检查和调查，现场检查和调查时间应不少于45天。

5.审计组应通过调阅资料、访谈人员、实地查看等方式全面了解有关情况，对发现的问题进行取证，并对获取的审计证据进行鉴定、整理和分析，对于审计对象有异议的应进一步核实，当证据之间存在矛盾时，应搜集更多证据进行判断，保证审计证据的相关性、可靠性和充分性。

6.审计过程中应坚持文明审计，与被审计单位及相关人员沟通应以理服人、平等待人，并遵守公司工作秩序和社会道德。

7.审计组应根据检查情况、审计发现及取得的证据，按照公司内部审计制度要求格式编写审计事实确认书，由审计对象确认。审计组完成事实确认等必要的审计程序后，应就审计事项做出审计结论、提出审计意见和建议，形成审计报告，报公司审计部复核。审计报告内容、格式应遵循公司内部审计制度相关要求。审计组应收集整理审计全过程的资料，移交公司审计部归档。服务商应对审计实施质量，以及审计证据、审计工作底稿、审计事实确认书、审计报告的总体质量，以及移交资料的完整性负责。

11.审计全程用时不应超过3个月，其中审计报告初稿应在2.5个月内完成，以确保在总体时限内完成审计报告向被审计单位征求意见及公司内部审批。

12.公司审计部负责全过程跟踪，协调被审计单位及人员配合审计，对审计过程进行监督，对审计成果及重要过程文档进行质量控制。

13.服务商及审计组人员应严格履行保密责任，不得私自留存、拷贝、非法获取、泄露审计过程中取得的资料或信息。

### 三、项目服务期

合同签订后采购人通知开始日起不超过3个月内完成项目审计工作（其中审计报告初稿应在2.5个月内完成；驻场工作时间不低于45天），并出具项目审计报告作出审计结论和建议。

### 四、付款方式

按照国银金融租赁股份有限公司相关规定执行。中标人须提供相应的增值税专用发票。

### 五、注意事项

1、中标人不得将项目非法分包或转包给任何单位和个人。否则，国银金融租赁股份有限公司有权即刻终止合同，并要求中标人赔偿相应损失。

2、供应商若认为磋商文件的技术要求或其他要求有倾向性或不公正性，可在磋商答疑阶段提出，以维护招标行为的公平、公正。

### 六、项目报价注意事项

1、供应商应根据本企业的成本自行决定报价，但不得以低于其企业成本的报价投标； 供应商报价必须充分考虑到管理服务要求和特点，以及服务的各种管理因素和环境条件，在资源配置方面必须满足现有服务需求，并能够保持持续性改进提升的投入能力。中标人的报价包括入场的各项费用，本项目不再为此增加任何费用。

2、供应商的投标报价不得超过预算金额。

3、供应商的投标报价，应是本项目招标范围和磋商文件及合同条款上所列的各项内容中所述的全部，不得以任何理由予以重复，并以供应商在磋商响应文件中提出的综合单价或总价为依据。

4、中标人根据有关管理法规与国银金融租赁股份有限公司签订服务合同，对相关服务实行统一管理，综合服务，自主经营，自负盈亏。