

# 商业银行信息科技风险 现场检查指南

## 目 录

|                  |    |
|------------------|----|
| 第一部分概述           | 11 |
| 1. 指南说明          | 11 |
| 1.1 目的及适用范围      | 11 |
| 1.2 编写原则         | 12 |
| 1.3 指南框架         | 12 |
| 第二部分科技管理         | 13 |
| 2. 信息科技治理        | 13 |
| 2.1 董事会及高级管理层    | 14 |
| 检查项 1：董事会        | 14 |
| 检查项 2：信息科技管理委员会  | 14 |
| 检查项 3：首席信息官（CIO） | 14 |
| 2.2 信息科技部门       | 15 |
| 检查项 1：信息科技部门     | 15 |

- 检查项 2：信息科技战略规划 16
- 2.3 信息科技风险管理部门 16
  - 检查项 1：信息科技风险管理部门 16
- 2.4 信息科技风险审计部门 17
  - 检查项 1：信息科技风险审计部门 17
- 2.5 知识产权保护和信息披露 17
  - 检查项 1：知识产权保护 17
  - 检查项 2：信息披露 18
- 3. 信息科技风险管理 18
  - 3.1 风险识别和评估 18
    - 检查项 1：风险管理策略 18
    - 检查项 2：风险识别与评估 18
  - 3.2 风险防范和检测 19
    - 检查项 1：风险防范措施 19
    - 检查项 2：风险计量与检测 19
- 4. 信息安全管理错误!未定义书签。
  - 4.1 安全管理机制与管理组织错误!未定义书签。
    - 检查项 1：信息分类和保护体系错误!未定义书签。
    - 检查项 2：安全管理机制错误!未定义书签。
    - 检查项 3：信息安全策略错误!未定义书签。
    - 检查项 4：信息安全组织错误!未定义书签。
  - 4.2 安全管理制度错误!未定义书签。
    - 检查项 1：规章制度错误!未定义书签。
    - 检查项 2：制度合规错误!未定义书签。
    - 检查项 3：制度执行错误!未定义书签。
  - 4.3 人员管理错误!未定义书签。
    - 检查项 1：人员管理错误!未定义书签。
  - 4.4 安全评估报告错误!未定义书签。
    - 检查项 1：安全评估报告错误!未定义书签。
  - 4.5 宣传、教育和培训错误!未定义书签。
    - 检查项 1：宣传、教育和培训错误!未定义书签。
- 5. 系统开发、测试与维护错误!未定义书签。
  - 5.1 开发管理错误!未定义书签。
    - 检查项 1：管理架构错误!未定义书签。
    - 检查项 2：制度建设错误!未定义书签。
    - 检查项 3：项目控制体系错误!未定义书签。
    - 检查项 4：系统开发的操作风险错误!未定义书签。
    - 检查项 5：数据继承和迁移错误!未定义书签。
  - 5.2 系统测试与上线错误!未定义书签。

检查项 1: 系统测试错误!未定义书签。

检查项 2: 系统验收错误!未定义书签。

检查项 3: 投产上线错误!未定义书签。

5.3 系统下线错误!未定义书签。

检查项 1: 系统下线错误!未定义书签。

6. 系统运行管理错误!未定义书签。

6.1 日常管理错误!未定义书签。

检查项 1: 职责分离错误!未定义书签。

检查项 2: 值班制度错误!未定义书签。

检查项 3: 操作管理错误!未定义书签。

检查项 4: 人员管理错误!未定义书签。

6.2 访问控制策略错误!未定义书签。

检查项 1: 物理访问控制策略错误!未定义书签。

检查项 2: 逻辑访问控制策略错误!未定义书签。

检查项 3: 账号及权限管理错误!未定义书签。

检查项 4: 用户责任及终端管理错误!未定义书签。

检查项 5: 远程接入的控制错误!未定义书签。

6.3 日志管理错误!未定义书签。

检查项 1: 审计日志检查错误!未定义书签。

检查项 2: 日志信息的保护错误!未定义书签。

检查项 3: 操作日志的检查错误!未定义书签。

检查项 4: 错误日志的检查错误!未定义书签。

6.4 系统监控错误!未定义书签。

检查项 1: 基础环境监控错误!未定义书签。

检查项 2: 系统性能监控错误!未定义书签。

检查项 3: 系统运行监控错误!未定义书签。

检查项 4: 测评体系错误!未定义书签。

6.5 事件管理错误!未定义书签。

检查项 1: 事件报告流程错误!未定义书签。

检查项 2: 事件管理和改进错误!未定义书签。

检查项 3: 服务台管理错误!未定义书签。

6.6 问题管理错误!未定义书签。

检查项 1: 事件分析和问题生成错误!未定义书签。

检查项 2: 台账管理错误!未定义书签。

检查项 3: 问题处置错误!未定义书签。

6.7 容量管理错误!未定义书签。

检查项 1: 容量规划错误!未定义书签。

检查项 2: 容量监测错误!未定义书签。

检查项 3: 容量变更错误!未定义书签。

#### 6.8 变更管理错误!未定义书签。

检查项 1: 变更的流程错误!未定义书签。

检查项 2: 变更的评估错误!未定义书签。

检查项 3: 变更的授权错误!未定义书签。

检查项 4: 变更的执行错误!未定义书签。

检查项 5: 紧急变更错误!未定义书签。

检查项 6: 重大变更错误!未定义书签。

### 7. 业务连续性管理错误!未定义书签。

#### 7.1 业务连续性管理组织错误!未定义书签。

检查项 1: 董事会及高管层的职责错误!未定义书签。

检查项 2: 业务连续性管理组织的建立错误!未定义书签。

检查项 3: 业务连续性管理组织职责错误!未定义书签。

#### 7.2 IT 服务连续性管理错误!未定义书签。

检查项 1: IT 服务连续性计划的组织保障错误!未定义书签。

检查项 2: 风险评估及业务影响分析错误!未定义书签。

检查项 3: IT 服务连续性计划的制定错误!未定义书签。

检查项 4: IT 服务连续性计划的测试与维护错误!未定义书签。

检查项 5: IT 服务连续性计划审计错误!未定义书签。

检查项 6: IT 服务连续性相关领域的控制错误!未定义书签。

### 8. 应急管理错误!未定义书签。

#### 8.1 应急组织错误!未定义书签。

检查项 1: 应急管理团队错误!未定义书签。

检查项 2: 应急管理职责错误!未定义书签。

检查项 3: 应急管理制度错误!未定义书签。

#### 8.2 应急预案错误!未定义书签。

检查项 1: 应急预案制订错误!未定义书签。

检查项 2: 应急预案内容错误!未定义书签。

检查项 3: 应急预案更新错误!未定义书签。

检查项 4: 外包服务应急错误!未定义书签。

检查项 5: 应急预案培训错误!未定义书签。

#### 8.3 应急保障错误!未定义书签。

检查项 1: 人员保障错误!未定义书签。

检查项 2: 物质保障错误!未定义书签。

检查项 3: 技术保障错误!未定义书签。

检查项 4: 沟通保障错误!未定义书签。

8.4 应急演练错误!未定义书签。

检查项 1: 应急演练的计划错误!未定义书签。

检查项 2: 应急演练的实施错误!未定义书签。

检查项 3: 应急演练的总结错误!未定义书签。

8.5 应急响应错误!未定义书签。

检查项 1: 应急响应流程错误!未定义书签。

检查项 2: 全程记录处置过程错误!未定义书签。

检查项 3: 应急事件报告错误!未定义书签。

检查项 4: 与第三方沟通错误!未定义书签。

检查项 5: 向新闻媒体通报制度错误!未定义书签。

检查项 6: 应急处置总结错误!未定义书签。

8.6 持续改进错误!未定义书签。

检查项 1: 应急事件评估错误!未定义书签。

检查项 2: 应急响应评估错误!未定义书签。

检查项 3: 应急管理改进错误!未定义书签。

9. 灾难恢复管理错误!未定义书签。

9.1 灾难恢复组织架构错误!未定义书签。

检查项 1: 灾难恢复相关组织架构错误!未定义书签。

9.2 灾难恢复策略错误!未定义书签。

检查项 1: 总体控制错误!未定义书签。

检查项 2: 灾难恢复策略错误!未定义书签。

检查项 3: 灾难备份策略错误!未定义书签。

检查项 4: 外包风险错误!未定义书签。

9.3 灾难恢复预案错误!未定义书签。

检查项 1: 灾难恢复预案错误!未定义书签。

检查项 2: 联络与通讯错误!未定义书签。

检查项 3: 教育、培训和演练错误!未定义书签。

9.4 评估和维护更新错误!未定义书签。

检查项 1: 灾备策略的评估和维护更新错误!未定义书签。

检查项 2: 灾难恢复预案的评估和维护更新错误!未定义书签。

10. 数据管理错误!未定义书签。

10.1 数据管理制度和岗位错误!未定义书签。

检查项 1: 数据管理制度错误!未定义书签。

检查项 2: 数据管理岗位错误!未定义书签。

10.2 数据备份、恢复策略错误!未定义书签。

检查项 1: 数据备份、转储策略错误!未定义书签。

检查项 2: 数据恢复、抽检策略错误!未定义书签。

10.3 数据存储介质管理错误!未定义书签。

检查项 1: 介质管理错误!未定义书签。

检查项 2: 介质的清理和销毁错误!未定义书签。

11. 外包管理错误!未定义书签。

11.1 外包管理制度错误!未定义书签。

检查项 1: 外包管理制度错误!未定义书签。

检查项 2: 外包审批流程错误!未定义书签。

检查项 3: 外包协议错误!未定义书签。

检查项 4: 服务水平协议错误!未定义书签。

检查项 5: 外包安全保密措施错误!未定义书签。

检查项 6: 外包文档管理错误!未定义书签。

11.2 外包评估和监督错误!未定义书签。

检查项 1: 外包服务商的评估错误!未定义书签。

检查项 2: 外包项目的监督管理错误!未定义书签。

12. 内部审计错误!未定义书签。

12.1 内部审计管理错误!未定义书签。

检查项 1: 内部审计部门、岗位、人员和职责错误!未定义书签。

检查项 2: 内部审计制度和办法错误!未定义书签。

12.2 内部审计要求错误!未定义书签。

检查项 1: 内部审计范围和频率错误!未定义书签。

检查项 2: 内部审计结果的有效性错误!未定义书签。

13. 外部审计错误!未定义书签。

13.1 外部审计资质错误!未定义书签。

检查项 1: 外部审计机构的资质错误!未定义书签。

13.2 外部审计要求错误!未定义书签。

检查项 1: 商业银行配合外部审计情况错误!未定义书签。

检查项 2: 外部审计有效性错误!未定义书签。

检查项 3: 外审过程中的保密要求错误!未定义书签。

第三部分基础设施错误!未定义书签。

14. 计算机机房错误!未定义书签。

14.1 计算机机房建设错误!未定义书签。

检查项 1: 计算机机房选址错误!未定义书签。

检查项 2: 机房功能分区错误!未定义书签。

检查项 3: 计算机机房基础设施建设错误!未定义书签。

检查项 4: 计算机机房的环境要求错误!未定义书签。

检查项 5: 计算机机房日常维护错误!未定义书签。

14.2 计算机机房管理错误!未定义书签。

检查项 1: 计算机机房安全管理错误!未定义书签。

检查项 2: 计算机机房集中监控系统错误!未定义书签。

检查项 3: 计算机机房安全区域访问控制错误!未定义书签。

检查项 4: 计算机机房运行管理错误!未定义书签。

#### 14.3 机房设备管理错误!未定义书签。

检查项 1: 机房设备的环境安全错误!未定义书签。

### 15. 网络通讯错误!未定义书签。

#### 15.1 内控管理错误!未定义书签。

检查项 1: 内控制度错误!未定义书签。

检查项 2: 人员管理错误!未定义书签。

检查项 3: 访问控制错误!未定义书签。

检查项 4: 日志管理错误!未定义书签。

检查项 5: 第三方管理错误!未定义书签。

检查项 6: 服务外包错误!未定义书签。

检查项 7: 文档管理错误!未定义书签。

检查项 8: 风险评估错误!未定义书签。

#### 15.2 网络运行维护错误!未定义书签。

检查项 1: 运行监控错误!未定义书签。

检查项 2: 性能监控错误!未定义书签。

检查项 3: 流量监控错误!未定义书签。

检查项 4: 监控预警错误!未定义书签。

检查项 5: 性能调优错误!未定义书签。

检查项 6: 事件管理错误!未定义书签。

检查项 7: 运行检查错误!未定义书签。

#### 15.3 网络变更管理错误!未定义书签。

检查项 1: 变更发起错误!未定义书签。

检查项 2: 变更计划错误!未定义书签。

检查项 3: 变更测试错误!未定义书签。

检查项 4: 变更审批错误!未定义书签。

检查项 5: 变更实施错误!未定义书签。

#### 15.4 网络服务可用性错误!未定义书签。

检查项 1: 容量管理错误!未定义书签。

检查项 2: 冗余管理错误!未定义书签。

检查项 3: 带外管理错误!未定义书签。

检查项 4: 压力测试错误!未定义书签。

检查项 5: 应急管理错误!未定义书签。

#### 15.5 网络安全技术错误!未定义书签。

- 检查项 1: 结构安全错误!未定义书签。
- 检查项 2: 物理安全错误!未定义书签。
- 检查项 3: 传输安全错误!未定义书签。
- 检查项 4: 访问控制错误!未定义书签。
- 检查项 5: 接入安全错误!未定义书签。
- 检查项 6: 网络边界安全错误!未定义书签。
- 检查项 7: 入侵检测防范错误!未定义书签。
- 检查项 8: 恶意代码防范错误!未定义书签。
- 检查项 9: 网络设备防护错误!未定义书签。
- 检查项 10: 网络安全测试错误!未定义书签。
- 检查项 11: 安全审计日志错误!未定义书签。
- 检查项 12: 安全检查错误!未定义书签。

16. 操作系统错误!未定义书签。

16.1 账号及密码管理错误!未定义书签。

- 检查项 1: 管理制度错误!未定义书签。
- 检查项 2: 账号、密码管理错误!未定义书签。
- 检查项 3: 账号、密码管理检查错误!未定义书签。

16.2 系统访问控制错误!未定义书签。

- 检查项 1: 访问控制策略错误!未定义书签。
- 检查项 2: 用户登录行为管理错误!未定义书签。
- 检查项 3: 登录失败日志管理错误!未定义书签。
- 检查项 4: 最小化访问错误!未定义书签。

16.3 远程接入管理错误!未定义书签。

- 检查项 1: 远程管理制度错误!未定义书签。
- 检查项 2: 远程维护管理错误!未定义书签。
- 检查项 3: 远程维护审查错误!未定义书签。

16.4 日常维护错误!未定义书签。

- 检查项 1: 系统性能监控错误!未定义书签。
- 检查项 2: 补丁及漏洞管理错误!未定义书签。
- 检查项 3: 日常维护管理错误!未定义书签。
- 检查项 4: 系统备份和故障恢复错误!未定义书签。
- 检查项 5: 病毒及恶意代码管理错误!未定义书签。
- 检查项 6: 定时进程设置管理错误!未定义书签。
- 检查项 7: 系统审计功能错误!未定义书签。

17. 数据库管理系统错误!未定义书签。

17.1 访问控制错误!未定义书签。

- 检查项 1: 身份认证错误!未定义书签。

检查项 2: 授权控制错误!未定义书签。

检查项 3: 远程访问错误!未定义书签。

检查项 4: 安全参数设置错误!未定义书签。

17.2 日常管理错误!未定义书签。

检查项 1: 数据安全错误!未定义书签。

检查项 2: 审计功能错误!未定义书签。

检查项 3: 性能管理错误!未定义书签。

检查项 4: 补丁升级错误!未定义书签。

17.3 连续性管理错误!未定义书签。

检查项 1: 备份和恢复错误!未定义书签。

检查项 2: 连续性和应急管理错误!未定义书签。

18. 第三方中间件错误!未定义书签。

18.1 产品管理错误!未定义书签。

检查项 1: 中间件测试错误!未定义书签。

检查项 2: 中间件管理错误!未定义书签。

检查项 3: 中间件与业务系统架构错误!未定义书签。

18.2 运行管理错误!未定义书签。

检查项 1: 维护流程和操作手册错误!未定义书签。

检查项 2: 中间件配置管理错误!未定义书签。

检查项 3: 中间件日志管理的程序错误!未定义书签。

检查项 4: 中间件的性能监控错误!未定义书签。

检查项 5: 中间件产生的事件和问题管理错误!未定义书签。

检查项 6: 中间件的变更错误!未定义书签。

检查项 7: 单点故障问题和负载均衡错误!未定义书签。

检查项 8: 压力测试错误!未定义书签。

第四部分应用系统错误!未定义书签。

19. 应用系统错误!未定义书签。

19.1 应用系统管理错误!未定义书签。

检查项 1: 业务管理办法与操作流程错误!未定义书签。

检查项 2: 重要应用系统评估错误!未定义书签。

检查项 3: 应用系统版本管理错误!未定义书签。

检查项 4: 应用系统培训教育错误!未定义书签。

19.2 应用系统操作错误!未定义书签。

检查项 1: 终端用户管理错误!未定义书签。

检查项 2: 访问控制与授权管理错误!未定义书签。

检查项 3: 数据保密处理错误!未定义书签。

检查项 4: 数据完整性处理错误!未定义书签。

- 5: 数据准确性处理错误!未定义书签。
- 检查项 6: 日志管理机制错误!未定义书签。
- 检查项 7: 备份、恢复机制错误!未定义书签。
- 检查项 8: 文档资料管理错误!未定义书签。
- 检查项 9: 内部审计的参与错误!未定义书签。
- 20. 电子银行错误!未定义书签。
  - 20.1 电子银行业务合规性错误!未定义书签。
    - 检查项 1: 电子银行业务合规性错误!未定义书签。
  - 20.2 电子银行风险管理体系错误!未定义书签。
    - 检查项 1: 电子银行风险管理体系错误!未定义书签。
  - 20.3 电子银行安全管理错误!未定义书签。
    - 检查项 1: 电子银行安全策略管理错误!未定义书签。
    - 检查项 2: 电子银行安全措施错误!未定义书签。
    - 检查项 3: 电子银行安全监控错误!未定义书签。
    - 检查项 4: 电子银行安全评估错误!未定义书签。
  - 20.4 电子银行可用性管理错误!未定义书签。
    - 检查项 1: 电子银行基础设施错误!未定义书签。
    - 检查项 2: 电子银行性能监测和评估错误!未定义书签。
  - 20.5 电子银行应急管理错误!未定义书签。
    - 检查项 1: 电子银行应急预案错误!未定义书签。
    - 检查项 2: 电子银行应急演练错误!未定义书签。
- 21. 银行卡系统错误!未定义书签。
  - 21.1 银行卡系统管理错误!未定义书签。
    - 检查项 1: 银行卡系统容量的合理规划错误!未定义书签。
    - 检查项 2: 银行卡系统物理设备风险和故障处理错误!未定义书签。
    - 检查项 3: 银行卡交易监控错误!未定义书签。
    - 检查项 4: 账户密码和交易数据的存储和传输错误!未定义书签。
    - 检查项 5: 银行卡系统应急预案错误!未定义书签。
  - 21.2 终端设备错误!未定义书签。
    - 检查项 1: 自助银行机具和安装环境的物理安全错误!未定义书签。
    - 检查项 2: 自助银行机具的通信安全错误!未定义书签。
    - 检查项 3: 自助银行机具的安全装置错误!未定义书签。
    - 检查项 4: 自助银行业务操作流程(机具软件)错误!未定义书签。
    - 检查项 5: 自助银行机具的巡查维护错误!未定义书签。
    - 检查项 6: POS机错误!未定义书签。
  - 21.3 自助银行监控错误!未定义书签。
    - 检查项 1: 自助银行设备日常运行的监控情况错误!未定义书签。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/225340122021011320>