金融业信息科技风险管理理念与实践

讲座人：梁力军

一. 讲座内容要点

一是信息科技风险管理规范标准。通过信息与资料梳理、视频素材分析，解析国际和国内金融业在信息系统风险控制、技术风险评级、信息安全和网络安全、系统安全和数据安全、信息科技项目管理、信息资产与基础设施、信息科技外包管理等方面的管理框架、行业标准和最佳实践，分析比较国际与国内金融业信息科技风险管理方面的特点、趋势和可借鉴之处。

二是信息科技风险管控实践。（1）从战略层面、战术层面和操作层面三个视角，分析国内外金融业信息科技治理结构的架构、信息科技管控流程的构建和信息科技系统管控的实施等；（2）从三道防线视角，即信息科技部门、信息科技风险管理部门、信息科技审计（稽核）部门，分析国内外金融业如何进行信息科技风险管控的有效协作、资源与信息共享、数据传递等；（3）从风险管理流程视角，分析国内外金融业如何实现对信息科技风险的感知与识别、评估与计量、应对等。

三是信息科技风险管控工具实践。以信息科技中信息系统与数据的“生命周期”为主线，从信息科技立项与需求分析、信息科技项目采购与招投标、信息科技项目开发、信息科技项目时间与质量管控、信息科技成本控制和资源管控、信息科技沟通管理、信息科技测试与运行等不同阶段讲解适用的各类信息科技风险管控工具与方法；从信息科技风险存在的不同载体——系统、设备、网络、数据和人员等视角，讲解防范信息系统单项风险和综合风险的工具与方法。

四是信息科技风险监管与审计实施。讲解国外金融业监管机构（巴塞尔委员会、COSO）、国内金融业监管机构（人民银行、银保监会、证监会）以及审计机构（国家审计署）和工信部等机构，实施信息科技风险监管和审计的具体标准和规范、实施要素和要点等。

二. 讲座主要价值点

一是以信息系统与数据“生命周期”为剖析主线，逻辑清晰。本讲座内容将针对信息科技治理、信息科技开发、信息科技测试、信息科技运维等不同阶段和环节，系统性、动态性的分析信息科技风险管理的特征与规律。

二是将信息科技风险管理的理论与实践相结合，理实结合。本讲座系统性的分析信息科技风险及风险管理的规范、行业标准、方法与工具、监管与审计的国际、国内前沿发展和最佳实践，并结合信息科技风险管理案例信息、视频素材、数据资料进行剖析讲解。

三是提出信息科技风险管理的实施体系与建议，具指导性。本讲座基于三道防线、生命周期，系统性提出金融机构实施信息科技风险管理的实施体系与建议方案，具有可操作性、指导性。

三. 讲座方案设计

本讲座设计为两天（12 小时）。

第一天：“规范标准篇”+“管理流程篇”

通过信息科技风险事件视频素材与态势分析，引出实施金融业信息科技风险管理的思考。

讲解和剖析国内外金融业信息科技风险管理的行业规范与标准，并提出适合于参训机构的、具可操作性的信息科技风险管理规范与标准。

从三个层面讲解国内外金融业信息科技风险管理实施的流程，并提出适合于参训机构的、具可操作性的信息管理流程。

第二天：“工具实践篇”+“监管审计篇”

以信息系统和金融数据的“生命周期”为主线，讲解不同阶段对应的信息科技风险管理工具与方法，并比较不同工具与方法的优劣。

讲解国内外金融监管机构的信息科技风险监管规范、监管科技工具、监管要求与要素等。

讲解国内外信息科技及风险管理的审计规范与准则、审计方法与审计工具、审计要素等。

四. 具体内容设计

(〇) 基础认知篇

1. 视频与案例素材剖析

 国外*IT 风险事件视频与案例剖析

 国内*IT 风险事件视频与案例剖析

2. 信息科技发展及 **IT** 风险

 信息科技发展对金融业的影响

 IT 风险内涵、种类与全域风险视图

 IT 风险的演进与变异

 IT 风险管控发展趋势

(一) 规范标准篇

1. 国外 **IT** 风险管控标准规范

 IT 服务管理：ISO20000 和 ITIL V3

 信息安全管理：ISO27001

 业务连续性管理：ISO22301

 ISACA: COBIT5

 DRI:业务连续性管理

2. 国内 **IT** 风险管控标准规范

 人民银行

 《银行业信息系统灾难恢复管理规范》

 《银行集中式数据中心规范》

 《网上银行系统信息安全通用规范》

 《金融行业信息系统信息安全等级保护》

 银保监会

 《商业银行信息科技风险管理指引》

 《银行业金融机构信息科技外包风险监管指引》

 《商业银行业务连续性监管指引》

 《银行业重要信息系统突发事件应急管理规范（试行）》

 《商业银行数据中心监管指引》

 《银行业金融机构重要信息系统投产及变更管理办法》

 其他相关规范

 网络安全法

 国家网信办、公安部、国家保密局、国家密码管理局

 关键基础设施风险评估

 网络安全等级保护

 《中华人民共和国突发事件应对法》

 GBT20988—2007《信息系统灾难恢复规范》

(二) 管理流程篇

1. IT 风险管理战略**/**战术**/**操作

 信息科技治理架构的构建与实施

 信息科技管控流程的构建与实施

 信息科技管控系统的构建与实施

2. **IT** 风险管理三道防线

 信息科技部门职责与协作

 信息科技风险管理部门职责与协作

 信息科技审计部门职责与协作

3. **IT** 风险管理流程与系统构建

 信息科技风险感知与识别

 信息科技风险评估

 信息科技风险计量

 信息科技风险监测

 信息科技风险应对

 信息科技风险管理系统构建

(三) 工具实践篇

1. 信息系统与金融数据生命周期

 信息系统**/**项目生命周期各阶段划分

 金融数据生命周期各阶段划分

2. 各阶段 **IT** 风险管理工具与方法

 信息科技需求与设计阶段**/**案例解析

 信息科技项目立项阶段**/**案例解析

 信息科技开发与测试阶段**/**案例解析

 信息科技运行与维护阶段**/**案例解析

 信息科技外包阶段**/**案例解析

 业务连续性管理**/**案例解析

3. 单项与综合 **IT** 风险管理工具

 系统与设备安全方面/案例解析

 网络安全方面/案例解析

 数据安全方面/案例解析

 人员与操作风险方面/案例解析

4. **IT** 风险管控方案建议

(四) 监管审计篇

1. 国内外 **IT** 监管实施情况**.**

 巴塞尔委员会、COSO 监管情况

 人民银行、银保监会等监管情况

2. 国内外 **IT** 审计实施情况

 国外信息科技审计实施及案例

 国内信息科技审计实施及案例

3. IT 监管与 **IT** 审计实施借鉴

五. 讲座目的

本讲座通过系统讲解金融业（包括人民银行、银保监部门、商业银行、证券业及保险业等）信息科技风险管理体系与框架、信息管理科技风险特征与分布、信息科技风险的生命周期追踪、信息科技风险管理具体技术及方法、信息科技风险治理、信息科技风险监管等方面的最新发展和最佳实践，提出适合于参训机构实施信息科技风险管理的实施方案和体系建议，有效提升参训机构的信息科技风险管理能力。工具、营销策略，全面提升商业银行零售金融的营销能力。

本讲座内容适合但不限于金融从业机构、监管机构、类金融机构和互联网企业等的信息科技、风险管理、内控与审计等部门及相关职能部门的专业人员和银行从业人员。具体可包括：

 分管信息科技、科技风险的高级管理人员

 信息科技部门相关负责人

 风险管理部门相关人员

 信息科技部门管理和业务骨干等