附件一

银行业金融机构信息科技风险评估指南

（2011 版）

目录

第一章 总则

1.1 目的

为规范银行业金融机构信息科技非现场风险评估工作，建立有效的信息科技风险评估指标体系及风险评估方法，依据《中华人民共和国银行业监督管理法》、《中华人民共和国商业银行法》、《中国银行业监督管理委员会信息科技非现场监管指引（试行）》、《商业银行信息科技风险监管指引》和其他相关法律、法规，制定本指南。本指南主要目的包括:

1. 建立一套完整、合理、开放的信息科技风险评估指标及评估方法，以求客观反映银行业金融机构信息科技风险现状及管控水平，为各级监管部门全面开展信息科技风险非现场监管工作提供参考和指导。

2. 坚持以风险导向监管的原则，全面、持续地识别、监测、分析、评估机构信息科技风险，提高各级监管部门信息科技风险信息采集和分析能力，采取具有针对性的监管措施，提高信息科技风险非现场监管效率。

3. 为后续实现对银行业金融机构信息科技风险的持续监管、分类监管和风险预警，以及推行同质同类银行业金融机构比较和差别监管模式等监管评价、评级工作提供参考和依据，以此形成有效的信息科技风险日常监管机制，及时纠正和制止危及银

行业金融机构健康发展的风险因素，保障信息科技安全、稳健运行。

4. 进一步将信息科技风险纳入银监会全面风险监管框架，以识别、评估、监测和控制银行业金融机构信息科技风险为主线，通过信息科技风险识别与综合风险评价相结合，现场检查与非现场监管相结合，客观数据与主观判断相结合等方式方法，逐步丰富和完善信息科技风险非现场监管体系。

本指南主要内容包括:

1. 信息科技风险评估框架

2. 信息科技风险评估指标

3. 信息科技风险评估方法

银监会及其派出机构信息科技监管部门应利用本指南中的监管指标及评估方法，定期或不定期开展银行业金融机构机构信息科技风险信息收集和风险评估工作。

1.2 适用范围

本指南主要适用于中国银行业监督管理委员会（以下简称银监会）及其派出机构对在中华人民共和国境内依法设立的法人银行业金融机构（以下简称机构）进行信息科技风险评估。

第二章 信息科技风险评估框架

本指南所指信息科技风险非现场监管是指非现场监管人员按照风险为本的监管理念，全面、持续的收集和分析机构的信息科技固有风险和控制信息，分析、评估信息科技风险水平，制定监管计划合理配置监管资源，并实施一系列分类监管措施的周而复始的过程。信息科技风险评估框架如图 1 所示：

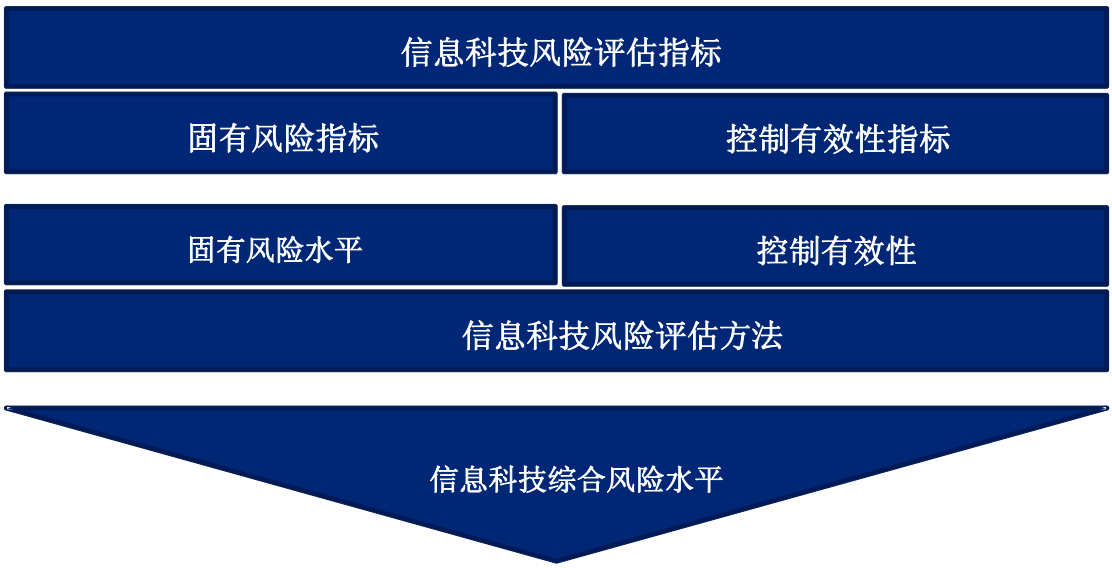

图 1：信息科技风险评估框架

上述框架主要由信息科技风险评估指标以及信息科技风险评估方法两部分内容构成。

2.1 信息科技风险评估指标

信息科技风险评估指标（以下简称评估指标）是在监管工作中定期或不定期使用的，具有可比性的，可反映机构信息科技现状和风险水平的一系列判断结果、数值或比率。

评估指标分为固有风险维度和控制有效性维度。

固有风险维度由风险子领域、评估指标和参考评估标准三部分组成。监管人员通过定量和定性分析，识别、评估机构信息科技固有风险水平。

控制有效性维度包括控制子领域、评估指标和参考评估标准三部分。监管人员通过定量和定性分析，评估机构信息科技控制有效性。

本指南主要采用定量和定性两类指标对信息科技风险进行分析。定量指标结果是一个正数，它有可能是某个正数区间范围内的任何一个数值，指标得分根据指标结果区间给出。定性指标结果基于报送数据、日常风险监测和现场检查掌握的情况，由监管人员参照评估标准逐项评判，按照机构实际情况与标准的符合程度给出指标得分。

具体评估指标详见附件一、二。

2.2 信息科技风险评估方法

信息科技风险评估方法是通过对信息科技风险种类、风险程度和风险发展趋势进行识别分析，对信息科技的风险状况、风险管理的充分性以及外部风险因素的影响做出判断，并在此基础上对机构的整体风险水平做出评估。

本指南采用定性与定量相结合的方式开展信息科技风险评估工作。

信息科技风险评估方法主要包括以下内容:

（一）风险识别。信息科技监管人员基于银行业金融机构信息科技非现场监管报表，以及其他各种渠道收集的信息技术发展态势、安全威胁、漏洞等信息，全面识别银行业金融机构面对的信息科技风险，并形成风险和控制清单。附件一、二根据当前银行业信息科技风险状况，给出了一份通用的固有风险和控制子领域评估清单。

（二）风险评估。本指南中的信息科技风险评估主要用于考量机构的信息科技综合风险水平。信息科技监管人员根据信息科技风险评估指标、计算方法、评判标准开展评估工作。信息科技风险评估分为信息科技固有风险水平评估和信息科技风险控制有效性评估两部分内容。机构整体信息科技风险水平按照公式：

【信息科技综合风险水平】=【固有风险】-【控制措施有效性】

得出。如有必要，信息科技监管人员可依据本指南开展信息科技某领域专项风险评估。

（三）风险分析。风险分析是对风险评估结果的进一步解析和确认。信息科技监管人员可以采取快速现场巡查、专题调研、专家会诊等多种方式方法，深入分析机构乃至行业中的突出信息科技风险成因，以利于制定有针对性的监管措施。

（四）基准分析。信息科技监管人员可基于所有银行业金融机构的风险评估结果，建立行业层面、地区层面、同质同类机构层面、信息科技专项领域层面的风险评估基准，并进一步构建信

息科技监管风险基线。

（五）评估报告。信息科技监管人员在风险评估和风险分析的基础上，分别撰写各机构信息科技风险评估报告，并根据机构信息科技风险水平高低，提出相匹配的监管意见和建议，合理分配监管资源。

第三章 风险评估指标

3.1 固有风险指标

固有风险是指在不考虑内部控制措施的前提下，由于内部因素和客观环境的影响，经营运作可能发生重大错误的风险。

信息科技固有风险是固有风险的重要组成部分，特指机构在信息技术的运用过程中所面对的固有风险。信息科技固有风险可以通过获取相关信息进行衡量和评价，其识别与评估是一个全面信息收集与综合分析研判的过程。

银行业是信息化高度集中的行业，尤其是实现了数据大集中的机构，信息技术贯穿于其日常经营的各个层面及环节，并承载了整个机构的日常运营。由于信息科技所具有的特殊属性，因其失效或缺陷所引发的风险中，除业务中断、交易出错、数据泄露等直接风险外，仍可能间接引发法律、声誉、操作等风险。

本指南主要通过重要信息系统、数据中心运行与灾备、信息科技项目、外包、系统恢复及数据保护 5 个子领域评估机构信息科技固有风险水平。通过对上述每一固有风险子领域进行根源分析，识别可能诱发该子领域固有风险事件的主要原因，作为其关键风险因素。每一关键风险因素由一组评估指标，按照一定的逻辑关系和运算方法进行度量。固有风险水平则通过对 5 个子领域的风险水平进行合成后得出。

具体的固有风险指标见附件一。

3.2 控制有效性指标

控制有效性是指机构所采用的信息科技风险控制措施的设计与执行效果满足监管机构和信息科技风险管理要求的程度。

控制的关键在于机构内部。监管机构应具备评估和判断机构所采取的控制措施是否有效的能力，并指导和监督机构持续改善信息科技治理和内控合规机制。

控制有效性主要通过信息科技治理、信息科技风险管理、信息科技审计、信息系统开发与测试、信息科技运行及维护、业务连续性管理、信息科技外包、信息安全 8 个子领域来评价。每一子领域控制有效性通过一组关键控制目标的有效性予以衡量，而每一关键控制目标可通过一组相应指标度量，并按照一定的逻辑关系和运算方法进行合成。整体控制有效性则通过 8 个子领域合成后得出。

具体的控制有效性指标见附件二。

第四章 风险评估方法

4.1 概述

信息科技风险评估是信息科技风险监管的核心步骤，旨在通过评估机构信息科技固有风险水平、信息科技风险控制措施有效性，对机构的整体风险状况进行评估。其作用是识别机构所面临的信息科技风险种类、信息科技风险水平以及信息科技风险管控能力。通过对机构的全面了解和主要信息科技风险、控制措施的识别、分析，分别完成对信息科技固有风险水平和控制有效性的评估，最后考察信息科技剩余风险。对于风险评估所识别出的高风险领域，可以作为监管机构现场检查的重点。根据现场检查的结果再对风险评估结果进行修正，如此循环往复，形成持续监管。

信息科技风险评估一般包括四个阶段：

1. 收集信息科技风险和控制措施信息；
2. 信息科技风险要素评估；
3. 信息科技风险分析；
4. 撰写信息科技风险评估报告。

4.2 固有风险评估

固有风险综合评分由评估指标、关键风险因素、风险子领域逐级计算得出。

（一）评估指标评分。根据给出的参考评估标准，对每一评

估指标进行评分。对于部分指标，参考评估标准可能不止一项，这里主要有两种情况，一种情况是适用性评估标准，需根据机构情况从列出的多项评估标准中选择对应的一项并据此得出指标评分；还有一种情况是综合性评估标准，所有列出的评估标准需综合考虑，即根据各项标准分别得出评分，最终取所有评分的最高值作为指标评分。评分时还需关注评估标准中是否有加分或扣分标准，如有应根据该项标准对指标评分进行适当调整。

为便于打分，指标评分采取 5 分制，得分区间为 0 分至 5 分。得出 5 分制评分后，再根据指标分值权重进行换算，得出指标得分，换算公式为：

指标得分 =（5 分制得分/5）*100%*指标分值权重，保留小数点后 2 位。

（二）关键风险因素得分。将各评估指标得分加总后得到关键风险因素得分。

（三）子领域评分。将各关键风险因素得分加总后得到风险子领域评分，满分为 100 分。

（四）固有风险评分。采用算术加权平均计算方法，将各风险子领域得分加权汇总，满分为 100 分，公式为：

固有风险得分=Σ(风险子领域得分*子领域权重)

（五）固有风险评估分级。根据固有风险得分，将固有风险评估结果分为低、中低、中高和高 4 级，每级又分为正（+）、负（-）2 个子级：

高+:　　80<固有风险得分<=100

高-:　　70<固有风险得分<=80

中高+:　60<固有风险得分<=70

中高-:　50<固有风险得分<=60

中低+:　40<固有风险得分<=50

中低-:　20<固有风险得分<=40

低+:　　10<固有风险得分<=20

低-:　　固有风险得分<=10

在评估过程中，以上固有风险等级划分标准可根据评估结果由银监会统一调整。

4.3 控制有效性评估

控制有效性评分是由评估指标、关键控制目标、控制子领域逐级计算得出。

（一）评估指标评分。参考评估标准，对每一评估指标进行评分。对于参考评估标准不止一项的指标，需根据机构情况从列出的多项评估标准中选择对应的一项并据此得出指标评分。同时还需关注评估标准中是否有加分或扣分标准，如有应根据该项标准对指标评分进行适当调整。

为便于打分，指标评分采取 5 分制，得分区间为 0 分至 5 分。得出 5 分制评分后，再根据指标分值权重进行换算，得出指标得分，换算公式为：

指标得分 =（5 分制得分/5）*100%*指标分值权重，保留小数点后 2 位。

（二）关键控制目标得分。将各评估指标得分加总后得到关键控制目标得分。

（三）子领域评分。将各关键控制目标得分加总后得到控制子领域评分，满分为 100 分。

（四）控制有效性评分。采用算术加权平均计算方法，对各个控制子领域进行加权汇总，公式为:

控制有效性得分=Σ(控制子领域得分*子领域权重)。

（五）控制有效性评估分级，根据控制有效性得分，将控制有效性评估结果分为弱、中弱、中强和强 4 级,每级又分为正(+)、负（-）2 个子级:

强+:　90<控制有效性得分<=100

强-:　80<控制有效性得分<=90

中强+:　70<控制有效性得分<=80

中强-:　60<控制有效性得分<=70

中弱+:　40<控制有效性得分<=60

中弱-:　30<控制有效性得分<=40

弱+:　20<控制有效性得分<=30

弱-:　控制有效性得分<=20

在评估过程中，以上控制有效性等级划分标准可根据评估结果由银监会统一调整。

4.4 综合评估

4.4.1 综合风险水平

本指南将信息科技综合风险水平分为六级。为体现同质同类机构之间的差距，其中 1 级、2 级和 3 级各分 a、b、c 三个子级，4 级、5 级和 6 级各分 a、b 二个子级，共计 15 个子级。信息科技综合风险水平由固有风险和控制有效性两个维度共同确定，评估时根据固有风险及控制有效性评估分级，对照综合评估矩阵，得出信息科技风险综合评估分级。

综合评估矩阵如下：

综合风险水平		控制有效性							
		强+	强-	中强+	中强-	中弱+	中弱-	弱+	弱-
固有风险	高+	3b	3c	4a	4b	5a	5b	6a	6b
	高-	3a	3b	3c	4a	4b	5a	5b	6a
	中高+	2c	3a	3b	3c	4a	4b	5a	5b
	中高-	2b	2c	3a	3b	3c	4a	4b	5a
	中低+	2a	2b	2c	3a	3b	3c	4a	4b
	中低-	1c	2a	2b	2c	3a	3b	3c	4a
	低+	1b	1c	2a	2b	2c	3a	3b	3c
	低-	1a	1b	1c	2a	2b	2c	3a	3b

4.4.2 综合评估结论

信息科技风险综合评估结果得出后，信息科技监管人员应当对机构总体信息科技风险状况进行权衡，在综合考虑固有风险水平、控制有效性及风险发展趋势的基础上，对综合评估分级结果进行验证和调整，并给出综合评估结论。

各类机构信息科技情况复杂，彼此之间差异较大，监管人员

应审慎对待综合评估结果。评估时应当分析和复核综合风险评估卡中各项子领域中是否存在得分过于极端的单项，如有必要，应对综合评估结果适当调整。

风险评估是一个动态过程，如果遇到重大情况或突发事件对机构的信息科技风险及其管理带来重大影响时，应及时对机构重新开展风险评估。现场检查结束后，如有必要，可根据现场检查结果对机构的信息科技风险水平进行调整。此外，监管人员在对风险进行评估时，需要考虑未来一段时期（如未来 12 个月）信息科技风险变化趋势，使风险评估不仅能够反映机构目前风险现状，而且能够对风险发展趋势做出前瞻性预测。判断风险发展趋势需要分析所有影响机构信息科技风险状况的关键因素，包括业务或信息科技战略变化、重要人事变动、重要信息系统投产或重大变更、风险管理体系和内部控制重大变化。

综合评估结论主要是对信息科技风险水平、监管意见进行描述，描述时可参考附件三。同时，综合评估结论还应对固有风险较高的领域和控制有效性较弱的领域进行简要描述。

4.4.3 综合评估卡

综合评估卡用于记录信息科技风险结果以及评估结论，通过该卡反映一个机构的信息科技风险概况。

固有风险	固有风险得分		评估人	
	重要信息系统		数据中心运行与灾备	
	信息科技项目		信息科技外包	

	系统恢复及数据保护		固有风险调整后得分	
控制有效性	控制有效性得分		评估人	
	信息科技治理		信息科技风险管理	
	信息科技审计		信息系统开发与测试	
	信息科技运行及维护		业务连续性管理	
	信息科技外包		信息安全	
综合评估	固有风险分级		控制有效性分级	
	综合风险水平		评估人	
	综合评估结论			

4.5 撰写风险评估报告

信息科技监管人员通过风险矩阵分析和归纳，识别出高风险和控制薄弱领域后，应撰写信息科技风险评估报告，从风险导向角度综合分析一家机构，勾勒其风险轮廓和监管者关注的风险点，为下一步监管行动提供依据。

信息科技风险评估报告应当包含以下内容:

1.机构的总体风险评估结果，固有风险水平和控制有效性的简要描述;

2.按固有风险领域描述综合固有风险评估结果，并对得分在4分以上的指标进行分析，指出高风险指标和领域;

3.按控制措施领域描述机构的控制措施有效性，并对得分在2分以下的指标进行分析，指出控制较弱的指标和领域;

4.在各固有风险水平、控制措施有效性的描述中，要根据重要性原则，突出描述产生重要风险的职能部门、处室或服务活动，

以及可能影响机构信息科技风险状况的关键问题;

5.在描述风险时，要综合考虑发生不利事件的可能性及其发生对机构的影响程度。

信息科技风险评估报告最初虽然是出于监管规划的目的撰写，但作为风险导向监管的核心文件，应随时根据所掌握的信息进行更新。比如在现场检查后，就要根据检查结果对风险评估的细节进行修正，在机构发生业务系统、人员、组织架构等方面的变动后，也应及时更新，以保证持续有效的评估。

附件一 固有风险指标

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
重要信息系统(KS) 权值：34%	重要信息系统重大变动（分值：30）	1	KS01	核心业务系统替换。 机构在近期已实施或将实施核心业务系统替换，可能影响所有业务系统。	1．新的核心系统已经开发完成，过去 12 个月进行系统上线实施工作（评估分值保留小数点后 2 位，下同）：	参考 T-B-7 第 13 项及日常风险监测情况	16
					（1）已全部完成，且上线过程中未出现异常，【1-3】分		
					（2）全部完成，但过程中出现异常，【2-4】分		
					（3）已部分完成上线，得分区间【3-5】分		
					2．过去 12 个月正在进行新的核心系统开发工作，尚未正式上线：		
					（1）项目按计划进度进行的，【1-2】分		
					（2）项目延期 6 个月以内的，【2-3】分		
					（3）项目延期 6 个月以上的，【3-5】分		
					（4）过去 12 个月发生核心系统项目关键人员、外包机构、技术架构、项目计划重大变更的，风险得分酌情增加【1-2】分		
					3．新核心系统已开发完成或进入收尾阶段，未来 12 个月计划新核心系统上线，【2-4】分。		
					4．未来 12 个月计划启动新核心系统替换开发项目，【1-3】分。		
		2	KS02	重要信息系统紧急变更。 重要信息系统紧急变更过多反映机构在变更管理方面存在较多非计划因素，如：系统存在未被发现的缺陷等。存在变更失误导致影	1．根据重要信息系统紧急变更率（＝重要信息系统紧急变更数/重要信息系统变更总数*100%）：	参考 T-B-7 第 12 项	6
					（1）【75，100】，【4-5】分		
					（2）【50，75】，【3-4】分		
					（3）【25,50】,【2-3】分		
					（4）【5，25】，【1－2】分		

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
				响业务稳定运行的风险。	（5）【0，5】，【0－1】分		
		3	KS03	重要信息系统重大变更。重大变更包括：新的重要信息系统投产（或重要信息系统大版本投产）；重要信息系统启用新的操作系统、数据库、中间件等系统平台等情况。信息系统重大变更初期，问题较频繁和集中，是可能影响业务稳定运行的重要因素之一。	1．评估期内，重要信息系统重大变更数量比上一评估期增长： （1）【50%,100%】，【3－5】分 （2）【30%-50%】，【2－3】分 （3）【0－30%】，【0－2】分 2．评估期内，因生产环境变更引发异常事件,视事件数量和严重程度酌情增加【2－3】分； 注：核心业务系统替换、数据中心设立、迁移等重大变更已另项评估，本项所指是除核心业务系统替换及数据中心设立迁移以外的重要信息系统重大变更。	参考T-A-6，T-B-7 附件重要信息系统情况明细报告	8
	重要信息系统复杂度（分值：30）	4	KS04	重要信息系统系统外联度。外联系统数量过多将增加系统复杂度，同时可能存在信息安全问题。	1．外联系统情况： （1）具有银证、银期、银行卡等与外部实时交易连接的重要信息系统，且此类连接机构占全部外联机构 50%以上，【4－5】分 （2）具有银证、银期、银行卡等与外部实时交易连接的重要信息系统，且此类连接机构占全部外联机构 50%以下，【3－4】分 （3）其他，【0－3】分 2．外联行业和外联机构数： （1）外联行业 15 个以上，或外联机构数 100 个以上，【4-5】分 （2）外联行业【10-15】个，或外联机构 50 个以上，【3-4】分 （3）外联行业【5-10】个，或外联机构 30 个以上，【2-3】分 （4）外联行业 5 个以下，或外联机构 30 个以下，【1-2】分 （5）无外联机构，0 分	参考 T-B-7 第 10 项及日常风险监测情况	10

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
		5	KS05	电子银行依赖程度。 网上银行、手机银行、自助银行等电子银行渠道的普及使银行机构的信息系统直接面对复杂的公共网络环境。	1．电子银行业务品种：个人网银、企业网银、自助银行、电话银行、手机银行：	参考 T-B-8、T-Q-4	20
					（1）含有个人网银、企业网银 【3-5】分，仅有个人网银或企业网银【2－4】分		
					（2）有手机银行，酌情增加【1－2】分		
					（3）有自助银行、电话银行，酌情增加【1-2】分		
					2．主要电子交易笔数替代率：		
					（1）【80－100】，【4－5】分		
					（2）【60－80】，【3－4】分		
					（3）【40－60】，【2－3】分		
					（4）【20－40】，【1－2】分		
					（5）【0，20】，【0－1】分		
					3．主要电子交易金额替代率：		
					（1）【80－100】，【4－5】分		
					（2）【60－80】，【3－4】分		
					（3）【40－60】，【2－3】分		
					（4）【20－40】，【1－2】分		
					（5）【0，20】，【0－1】分		
					4．网上银行交易笔数替代率超过 50%，加【0－1】分		
	重要信息系统的稳定性（分	6	KS06	重要信息系统平台环境。 服务器、操作系统、数据库、中间件等构成重要信息系统运行的平台环境。机构继	1．使用已停止支持的硬件平台系统占比：	参考 T-B-7 附件重要信息系统情况明细报告，	15
					（1）【80，100】，【4－5】分		
					（2）【60－80】，【3－4】分		
					（3）【40－60】，【2－3】分		

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
	值：40）			续沿用已过时（淘汰）软、硬件技术，发生故障时，可能难以及时获得供应商有效地支持，从而影响业务连续运行。此外，使用多种操作系统、数据库、中间件技术平台也加大了系统的复杂度。	（4）【20－40】，【1－2】分	T-B-13	
					（5）【0，20】，【0－1】分		
					2．使用已停止支持的软件平台的系统占比：		
					（1）【80，100】，【4－5】分		
					（2）【60－80】，【3－4】分		
					（3）【40－60】，【2－3】分		
					（4）【20－40】，【1－2】分		
					（5）【0，20】，【0－1】分		
					3．硬件、数据库、中间件平台，视异构平台数量，酌情加分：		
					（1）异构硬件平台达到 5 种以上，加【1-2】分		
					（2）数据库平台达到 3 种以上，加【0-1】分		
					（3）中间件平台达到 3 种以上，加【0-1】分		
					4．系统平台软件如有非授权软件，视非授权软件装机量、所服务的信息系统重要性，【3-5】分		
		7	KS07	渠道管理类重要信息系统。渠道管理类重要信息系统通常具有直接面向客户、实时性要求高、地域跨度大、影响面广等特点。	1．考察渠道类重要信息系统数量占比：	参考 T-B-7 第 2 项，附件重要信息系统情况明细报告，T-B-1 第 10 项	25
					（1）【80，100】，【4－5】分		
					（2）【60－80】，【3－4】分		
					（3）【40－60】，【2－3】分		
					（4）【20－40】，【1－2】分		
					（5）【0，20】，【0－1】分		
					2．考察渠道类重要信息系统高可用措施：		
					（1）全部未采用高可用措施，【4-5】分		
					（2）部分采用高可用措施，【2-4】		

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
					3.经营地域分布		
					本地市（县）经营 1 分，跨地市经营 1 分、跨省经营 2 分、跨境经营 1 分，本项得分为上述几项得分之和，最低 1 分，最高 5 分。		
					4.机构网点规模		
					（1）5000 以上，【4-5】分		
					（2）【1000，5000】，【3-4】分		
					（3）【300-1000】，【2-3】分		
					（4）300 以下，【1-2】分		
数据中心运行与灾备(DC) 权值：20%	数据中心的重大变动（分值：30）	8	DC01	数据中心基础设施重大变更。 数据中心承载了所有生产系统的运行，其重大变更对生产系统的影响在较长时间内难以完全消除。重大变更主要包括：数据中心、灾备中心地理位置变动，中心机房全面整改，网络架构、主机架构、应用架构重大调整等。	数据中心含生产中心和灾备中心。对未设立数据中心的机构，需考察机房变动情况。	参考 T-B-6 、T-A-4	30
					1．过去 12 个月新设立生产中心并实施迁移，未出现运行异常，【1－3】分；出现运行异常【3－5】分；		
					2.过去 12 个月新设立同城灾备中心或异地灾备中心，未出现运行异常【1－2】分，出现运行异常【2－4】分；		
					3．过去 12 个月实施数据中心改造，未出现异常【1－3】分；出现异常【3－5】分。		
					4．关键基础设施变更：		
					（1）发生网络架构重大变更的，【3－5】分		
					（2）发生存储架构重大变更的，【3－5】分		
					（3）生产中心机房重大改造，【3－5】分		
					（4）主机架构重大变更，【2－5】分		
					（5）其他关键基础设施变更，视情况酌情增加【1－2】分		
	数据中心与灾	9	DC02	数据中心（含灾备中心）所在地自然和社会环境。	1．数据(灾备)中心所在地评估期内发生过大型自然灾害，如：火灾、水灾、泥石流、地震、台风等，造成数据（灾备）中心损失的，【3-4】分；	参考 T-B-5 附件及日常	20

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
	备中心（场所）的分布状况（分值：20）				2．数据(灾备)中心所在地评估期内发生过大型自然灾害，但未造成损失的，【1-3】分；	风险监测情况	
					3．数据(灾备)中心所在地评估期内发生过群体性事件，【2－4】分；		
					4．数据(灾备)中心评估期内发生过人为破坏事件，如盗窃财物、线缆、非法闯入、内部人为破坏等事件的，视损失程度，【2-4】分。		
	公共基础设施状况（分值：50）	10	DC03	数据（灾备）中心电力供应。数据中心电力供应是数据中心平稳运行的基础。	1．双路市电接入：	参考T-B-6 、T-Q-1 第 7 项	20
					（1）生产中心无双路市电接入，【4-5】分；		
					(2)生产中心有双路市电接入,灾备中心不完全具备双路市电接入,【2-4】分；		
					（3）生产（灾备）中心全部都有双路市电接入，【1-2】分；		
					（4）对（2），（3）视双路接入是否由不同变电所接入，可酌情减【0-1】分。		
					2．UPS：		
					（1）UPS 供电模式存在单点，【4－5】分；		
					（2）实际负载峰值达到系统设计容量 70%的，【3-5】分；		
					（3）其他视供电模式、电池和主机服役年限酌情给予【0－3】分；		
					3．发电机：		
					（1）未配备发电机，【3－4】分；		
					（2）配备发电机，视自动启动、油料储备可用时间、运维单位情况酌情给予【0－3】分。		
					4．评估期内发生过数据中心市电中断		
					（1）中断 4 次（含）以上，【4－5】分		
					（2）中断【2-4】次，【2－4】分		

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
					（3）中断 2 次以下，【1-2】分		
					（4）如因市电中断导致 III 级以上信息科技突发事件，或最近一个季度市电中断次数上升，酌情加【1-2】分		
		11	DC04	核心网络系统。核心网络系统承载各类重要业务，其可靠性、稳定性具有全局影响。	1. 核心网络系统业务时段带宽占用情况（生产中心或中心机房到一级分支机构），重点考察评估期内最后一个季度的情况	参考 T-Q-1 第 3 项、第 7 项，T-B-9 第 3 项、第 4 项	20
					（1）80%以上，【4-5】分		
					（2）【50%-80%】之间，【2-4】分		
					（3）50%以下，【0-2】分		
					（4）如评估期内各季度带宽占用情况均在 80%以上，5 分		
					2.数据中心由于外部原因导致网络通讯中断次数		
					（1）中断 4 次（含）以上，【4－5】分		
					（2）中断【2-4】次，【2－4】分		
					（3）中断 2 次以下，【1-2】分		
					（4）如因数据中心网络中断导致 III 级以上信息科技突发事件，或最近一个季度网络中断次数上升，酌情加【1-2】分		
					3.生产网核心网络设备，包括核心路由器、核心交换机、核心网络安全设备存在单点，【3-5】分		
					4.生产网至一级分支机构、同城灾备中心、异地灾备中心线路冗余情况，存在线路单一或运营商单一的情况，【1-3】分		
		12	DC05	数据中心环境监控、防雷、放水、空调、消防等基础设施	1. 视环境监控覆盖程度，【0-3】分；	参考 T-B-6 第 3-8 项	10
					2. 不具备防雷设施，5 分；		
					3. 不具备防水设施，5 分；		
					4. 其他如空调、消防、巡检酌情【0-2】分。		

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
信息科技项目(PJ) 权值：10%	项目重大变更（分值：60）	13	PJ01	信息科技组织、人员是否发生重大变动。 信息科技组织、人员的重大变动对信息科技工作目标的达成可能产生影响。	1. 过去 12 个月发生过信息科技组织架构及人员重大变动：	参考 T-B-1 、T-A-1	30
					（1）信息科技相关部门（如：科技部、数据中心等）主要负责人变更，【3－5】分		
					（2）信息科技相关部门职能变更，【2－4】分		
					（3）关键岗位人员变动率，【80%-100%】，【4－5】分，【60%－80％】，【3－4】分，以此类推。		
					（4）机构信息科技战略、政策未发生重大变化，投入保持稳定，但信息科技正式员工出现下降，视下降幅度酌情增加【1－3】分。		
		14	PJ02	项目组织、人员情况。 重大项目的项目经理更换、质量保证人员的参与程度均可能影响项目进度和成果。	1.重大项目项目经理变更率＝重大项目项目经理变更人次/评估期内重大项目数：	参考 T-B-4 第 2 项	30
					（1）大于等于 50%，【4－5】分		
					（2）【30%－50%】，【2－4】分		
					（3）【10%-30%】，【1－2】分		
					（4）小于 10%，酌情【0－1】分		
	项目资源（分值：40）	15	PJ03	项目计划完成率。项目计划完成情况一定程度上反映了机构的项目管理能力和资源情况。	1. 年度项目计划完成率	参考 T-B-4 第 1 项	10
					（1）【80%－100%】，【0-1】分		
					（2）【50%-80%】,【1-3】分		
					（3）50%以下，【3-5】分		
		16	PJ04	发生延期的重大项目数。 需求变更、资源不足均有可能导致项目延期，而项目延期将影响业务投产安排、成本控制、资源调配等多方	1. 评估期内，发生延期的重大项目数占比：	参考 T-B-4 第 1 项	15
					（1）【80－100】，【4－5】分		
					（2）【60－80】，【3－4】分		
					（3）【40－60】，【2－3】分		
					（4）【20－40】，【1－2】分		

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
				面。	（5）【0－20】，【0－1】分		
		17	PJ05	软件开发项目工作量。软件开发项目工作量的增长会对项目资源造成压力。	1. 评估期内，软件开发项目工作量比上年增长幅度：	参考 T-B-4 第 1 项	15
					（1）超过 80%，【4－5】分		
					（2）【60%-80%】，【3－4】分		
					（3）【40%－60%】，【2－3】分		
					（4）【20%-40%】，【1－2】分		
					（5）20%以下，【0－1】分		
外包（OS）权值：12%	外包服务的稳定性（分值：20）	18	OS01	外包商、外包人员的异常退出直接影响外包工作的稳定性。外包人员变动过于频繁，可能会降低外包商的整体服务水平。	1. 外包人员异常退出率：	参考 T-B-16 第 2 项	20
					（1）50%(含)以上，【4-5】分		
					（2）【20%-50%】，【2-5】分		
					（3）20%以下，【1-2】分		
					2. 评估期内如发生过外包商异常退出事件（如：因破产退出市场、被竞争对手兼并等）并影响到服务稳定性的情况，且这种影响还将持续一段时间，视严重程度【2-4】分		
					3. 评估期内发生关键外包商更换，酌情增加【1－2】分		
					4. 评估期内发生外包引起的法律争议与诉讼，对外包服务产生影响，酌情增加【1-2】分		
	外包依赖程度（分值：60）	19	OS02	外包商数量。 外包商数量一定程度上反映机构对外包商的依赖程度以及相应的管理压力。	1. 外包商数量增长幅度（计算：评估期外包商数量-上一评估期外包商数量）/上一评估期外包商数量*100%）	参考 T-B-16 第 2 项	5
					（1）小于 20%（含负增长），【0-2】分		
					（2）【20%-50%】，【2-4】分		
					（3）50%以上，【4-5】分		
		20	OS03	外包项目情况。外包项目数	1. 外包项目增长幅度（计算：评估期外包项目数量-上一评估期外包项目	参考	10

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
				量反映机构对外包的依赖程度	数量）/上一评估期外包项目数量*100%）	T-B-16 第 1 项	
					（1）小于 20%（含负增长），【0-2】分		
					（2）【20%-50%】，【2-4】分		
					（3）50%以上，【4-5】分		
		21	0S04	外包范围。机构外包范围大小一定程度反映了机构对外包的依赖程度。特别是对重要信息系统和安全设施的外包，反映机构在核心科技能力方面对外包依存度较高。	1. 考察机构的外包范围：	参考 T-B-16 第 1 项	20
					（1）如包含数据中心运维、安全、加密产品运维外包，【3-5】分		
					（2）如包含开发、测试、应用系统运维，视外包程度和所涉及的信息系统的重要性【2-4】分		
					（3）仅包括硬件设备运维、桌面终端维护，【1-2】分		
		22	0S05	信息科技服务外包总工作量。 外包工作量一定程度反映机构信息科技对外部资源的依赖程度。	1. 评估期内，外包工作总量比上年增长幅度：	参考 T-B-16 第 1 项	15
					（1）超过 80%，【4－5】分		
					（2）【60%-80%】，【3－4】分		
					（3）【40%－60%】，【2－3】分		
					（4）【20%-40%】，【1－2】分		
					（5）20%以下，【0－1】分		
		23	0S06	现场执行开发任务的外包总工作量。 现场常驻外包人员数量一定程度反映机构系统开发对外部资源的依赖程度，并增加管理的复杂度。	1. 评估期内，软件开发外包项目工作量比上年增长幅度：	参考 T-B-4 第 1 项	10
					（1）超过 80%，【4－5】分		
					（2）【60%-80%】，【3－4】分		
					（3）【40%－60%】，【2－3】分		
					（4）【20%-40%】，【1－2】分		
					（5）20%以下，【0－1】分		

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
	外包商性质（分值：20）	24	OS07	外包商性质不同，机构的对外包商的管理和约束能力存在差异。重点考察数据中心、核心系统、渠道类（电子银行、银行卡等）领域的外包服务商。	1. 外包给境外母行或母公司：	参考T-B-16及附件，T-Q-2、T-Q-3	20
					（1）本行拥有独立的系统管理权限，且硬件、操作系统、数据库、应用实例与母行或母公司系统独立【2－3】分		
					（2）与母行或母公司共用硬件、操作系统，但数据库、应用实例独立，【3-4】分		
					（3）与母行或母公司共用硬件、操作系统、数据库、应用实例，【4－5】分		
					2. 外包给境外第三方机构，【4－5】分		
					3. 外包给境内母行或母公司：		
					（1）本行拥有独立的系统管理权限，且硬件、操作系统、数据库、应用实例与母行或母公司系统独立【1－2】分		
					（2）与母行或母公司共用硬件、操作系统，但数据库、应用实例独立，【2-3】分		
					（3）与母行或母公司共用硬件、操作系统、数据库、应用实例，【3－4】分		
					4. 外包给境内第三方机构，【2-4】分		
系统恢复及数据保护(SR)权值：24%	灾备基础设施（分值：35）	25	SR01	灾备基础设施外包。使用外部机构提供的共享灾难（应急）恢复设施，其业务持续能力和灾备设施可用性将主要依赖于外部机构及共同使用该设施的其它机构。	1. 使用外部机构提供的灾备设施，如：外部机构运营的灾备中心（机房），【3-5】分 2. 未使用外部机构提供的灾备设施，视灾备中心运维外包情况，【0-2】分	参考T-B-5	15
		26	SR02	交由外部机构托管的重要信息系统数。	1. 重要信息系统交由外部机构托管，托管的重要信息系统占比：	参考T-B-7第9项	20
					（1）【80－100】，【4－5】分		

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
				将重要信息系统交由外部机构托管，一方面反映机构科技运维能力不足，另一方面存在系统恢复时间取决于其他机构。	（2）【60－80】，【3－4】分		
					（3）【40－60】，【2－3】分		
					（4）【20－40】，【1－2】分		
					（5）【0－20】，【0－1】分		
					如托管系统涉及核心银行系统、渠道类（电子银行、银行卡等）重要信息系统，酌情增加【1-2】分		
	敏感数据保护（分值：45）	27	SR03	敏感数据处理外包。将涉及客户敏感信息（包括身份信息、账户信息、交易信息）的处理工作（如：客户信息录入、账单打印等）外包给第三方机构。	1. 如机构将敏感数据处理工作外包，视涉及的客户敏感信息数量、范围【3-5】分 2. 如无此类外包，0 分。	参考日常风险监测情况	15
		28	SR04	敏感数据潜在泄漏威胁。	1. 评估期内机构如开展过渗透性测试或对机构进行现场检查，发现存在敏感信息泄露的风险	参考 T-B-9 网络管理情况表及现场检查、渗透性测试报告	20
					（1）敏感信息存储在员工个人计算机设备，且未采取必要的防护措施，【3-4】分		
					（2）敏感信息可能通过网银系统、网站、网上商城等连接互联网的系统泄漏，【4-5】分		
					（3）内部渗透性测试发现安全漏洞，有可能从可从内部获取敏感信息，【3-4】分		
					（4）未开展渗透性测试，也未通过现场检查发现类似问题，但机构开办网上银行业务，有网上商城、网站等系统，且未在行内建立专门的敏感信息保护制度【2-3】分		

子领域	关键风险因素	序号	编码	指标	参考评估标准	数据来源	指标分值
		29	SR05	生产数据备份是否保存或托管于外部机构。 生产数据的备份介质或设备由本机构以外的实体保管或维护（例如，通过备份介质或在线方式进行异地备份），机构难以实施有效的控制。	1. 如机构将生产数据备份至外部机构，或者备份介质保存在外部机构，视外部机构的可控程度，【3－5】分 2. 无此类情况，0 分。	T-B-10 第 4 项	10
	突发事件情况（分值：20）	30	SR06	信息科技突发事件情况。机构在评估期内曾经发生过信息科技突发事件，暴露出其在业务连续性方面存在薄弱环节。	1. 评估期内，发生信息科技突发事件： （1）发生 I 级事件的，【4-5】分 （2）发生 II 级事件的，【3-4】分 （3）发生 III 级事件的，【2-3】分 （4）发生 III 级以下事件的，【1－2】分 视事件发生数量多少、影响程度在上述范围内评分，低等级事件如多次发生，也可上调其风险分值范围至上一等级。	参考 T-B-11，T-A-2	20

附件二 控制有效性指标

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
信息科技治理（G0）权重：15%	信息科技治理职责及运作情况（分值：40）	1	G0.01	董事会信息科技风险管理职责: 1.批准重大业务战略和科技战略； 2.确定风险管理策略、容忍度，包括信息科技风险管理容忍度（例如，可容忍的最大停机时间、可接受的最大损失金额等）； 3.及时向监管机构报告本机构重大信息科技事件； 4.审阅信息科技审计报告及信息科技风险评估报告； 5.监督信息科技内外审计整改的落实	1.未明确董事会信息科技风险管理职责【0】分	参考 T-B-1 第 2 项	9
					2.已明确董事会信息科技风险管理职责的机构，每包括下面一个职责加【0.6】分：		
					（1）批准重大业务战略和科技战略		
					（2）审批信息科技风险管理制度		
					（3）及时向监管机构报告本机构重大信息科技事件		
					（4）审阅信息科技审计报告及信息科技风险评估报告		
					（5）监督信息科技内外审计整改的落实		
					3.董事会（理事会）会议形成信息科技工作决议个数>=2 加【1-2】分		
		2	G0.02	设立首席信息官（CIO），直接向行长汇报，参与重大决策；CIO 应为机构高管，对本机构信息科技总体管理负责	1.未设立【0】分	参考 T-B-1 第 4 项	8
					2.已设立 CIO 得【3】分，已设立类似职务但名称不是首席信息官得【2】分		
					3.该职务纳入高级管理层，加【0-1】分		
					4.该职务汇报路线为直接向行长汇报，加【0-1】分		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
		3	G0.03	设立一个由来自高级管理层、信息科技部门和主要业务部门的代表组成的专门信息科技管理委员会，负责监督各项职责的落实	1.未设立【0】分 2.已设立【0-3】分 3.包括风险、计财和主要业务部门，加【0-1】分 4.成立信息科技管理委员会，定期或不定期召开会议决策信息科技管理重大事项，加【0-1】分	参考 T-B-1 第 3 项	9
		4	G0.04	内审部门设立专门的岗位负责信息科技内部审计，信息科技审计应当包括：落实信息科技审计制度和流程的实施，制订和执行信息科技审计计划，对信息科技整个生命周期和重大事件等进行审计	1.未设立信息科技内审岗位【0】分 2.已设立岗位，且配备专职人员，视岗位职责和专职人员数量【0-2】分 3.已设立岗位，并设置独立的信息科技内审处(科）室，视处（科）室职能和专职人员数量【3-5】分	参考 T-B-1 第 7 项	7
		5	G0.05	设立独立于信息科技风险管理部门（组织），承担信息科技风险管理责任，该部门负责协调制定有关信息科技风险管理制度(策略)，实施持续的信息科技风险评估，跟踪整改意见落实情况，监控信息安全威胁和信息科技风险事件的发生	1.未设立信息科技风险管理部门【0】分 2.已设立信息科技风险管理部门(组织)，但未独立于信息科技部门【0-3】分 3.已设立独立于信息科技部门的信息科技风险管理部门（组织）【3-5】分	参考 T-B-1 第 6 项	7
	信息科技战略	6	G0.06	具备评估和维护业务战略规划和信息科技战略规划	1.未建立信息科技战略规划【0】分 2.建立信息科技战略规划但未正式签发【1-2】分	参考 T-B-1 第 5 项	20

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
	及规划（分值：20）			一致性的机制	3.建立信息科技战略规划并正式签发【2-3】分		
					4.建立信息科技战略与业务战略的协调一致机制，加【0-1】分		
					5.信息科技战略规划内容包含的 5 个可选项，加【0-1】分		
					6.定期评价信息科技战略规划实施效果，加【0-1】分		
	信息科技管理制度（分值：40）	7	G0.07	建立信息科技制度管理流程，规范科技制度的起草、发布、修订等活动	1.未建立规范的制度起草、发布、修订工作流程【0】分	参考 T-B-1 第 8 项	5
					2.已建立规范的制度起草、发布、修订工作流程，但本年度新增、修订数量=0，【2-3】分		
					3.已建立规范的制度起草、发布、修订工作流程，且本年度新增、修订数量>0，【3-5】分		
		8	G0.08	建立完完整的信息科技风险管理体系	以下 3 项得分之和为指标得分：	参考 T-B-1 第 14 项及附件	5
					1.明确信息科技风险管理目标【0-1.5】分		
					2.建立信息科技风险评估方法和工作流程，并定期开展全面风险评估活动【0-2】分		
					3.建立信息科技风险监控预警指标体系【0-1.5】分		
		9	G0.09	建立完善的系统开发管理制度	衡量管理制度是否切实包含以下内容，以下 7 项得分之和为指标得分：	参考 T-B-1 第 14 项及附件	5
					1.需求管理【0-0.8】分		
					2.设计管理【0-0.7】分		
					3.编码管理【0-0.7】分		
					4.测试管理【0-0.7】分		
					5.验收管理【0-0.7】分		
					6.上线管理【0-0.7】分		
					7.软件配置管理（含版本管理及变更管理）【0-0.7】分		
		10	G0.10	建立完善的项目管理制度	衡量管理制度是否切实包含以下内容，以下 10 项得分之和为指标得分：	参考 T-B-1	5

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					1.项目立项审批管理【0-0.5】分	第 14 项及附件	
					2.项目综合管理【0-0.5】分		
					3.项目范围管理【0-0.5】分		
					4.项目时间管理【0-0.5】分		
					5.项目成本管理【0-0.5】分		
					6.项目质量管理【0-0.5】分		
					7.项目人力资源管理【0-0.5】分		
					8.项目沟通管理【0-0.5】分		
					9.项目风险管理【0-0.5】分		
					10.项目采购管理【0-0.5】分		
		11	G0.11	建立完善的系统运行管理制度	衡量管理制度是否切实包含以下内容，以下 8 项得分之和为指标得分：	参考 T-B-1 第 14 项及附件	5
					1.问题管理【0-0.6】分		
					2.事件管理【0-0.7】分		
					3.配置管理【0-0.6】分		
					4.变更管理【0-0.7】分		
					5.发布管理【0-0.6】分		
					6.日志管理【0-0.6】分		
					7.可用性管理【0-0.6】分		
					8.服务水平管理【0-0.6】分		
		12	G0.12	建立完善的信息安全管理制度	衡量管理制度是否切实包含以下内容，以下 10 项得分之和为指标得分：	参考 T-B-1 第 14 项及附件	5
					1.安全策略【0-0.5】分		
					2.安全事件管理【0-0.5】分		
					3.安全人员管理【0-0.5】分		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					4.安全资产管理【0-0.5】分		
					5.身份与访问管理【0-0.5】分		
					6.数据安全管理【0-0.5】分		
					7.应用安全管理【0-0.5】分		
					8.基础安全管理【0-0.5】分		
					9.密码技术管理【0-0.5】分		
					10.脆弱性管理【0-0.5】分		
		13	GO.13	建立完善的信息科技外包管理制度	衡量管理制度是否切实包含以下内容，以下 6 项得分之和为指标得分：	参考 T-B-1 第 14 项及附件	5
					1.外包策略【0-0.8】分		
					2.外包决策【0-0.9】分		
					3.外包供应商选择【0-0.8】分		
					4.供应商管理【0-0.8】分		
					5.合同管理【0-0.8】分		
					6.外包人员管理【0-0.9】分		
		14	GO.14	制定完善的业务连续性管理制度	衡量管理制度是否切实包含以下内容，以下 6 项得分之和为指标得分：	参考 T-B-1 第 14 项及附件	5
					1.业务连续管理目标【0-0.8】分		
					2.业务影响分析【0-0.9】分		
					3.应急管理【0-0.8】分		
					4.灾难恢复计划【0-0.9】分		
					5.业务连续性计划【0-0.8】分		
					6.培训及演练测试计划【0-0.8】分		
信息科技风险	信息科技风险	15	RM.01	风险管理部门中配置一定数量专职信息科技风险管	1.风险管理部门中未配备专职人员【0-1】分	参考 T-B-1 第 6 项	15
					2.风险管理职能部门中，未配备专职人员，但信息科技部门中配备有专职		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
管理（RM）权值：12%	管理人才（分值：30）			理人员	信息科技风险管理人员【1-3】分		
					3.风险管理职能部门中，配备信息科技风险管理专职人员，信息科技部门中也配备信息科技专职风险管理人员【3-5】分		
		16	RM.02	信息科技风险管理的人员具有相关专业背景知识和技能	1.风险管理职能部门中，未配备专职人员，或专职人员均无信息科技相关专业学历或工作经验【0-1】分	参考 T-B-1 第 13 项	15
					2.风险管理职能部门中，信息科技风险管理专职人员部分或全部具有信息科技相关专业学历或工作经验【1-3】分		
					3.风险管理职能部门中，信息科技风险管理专职人员均具有信息科技相关专业学历或工作经验，并且有一定数量人员获得信息科技高级专业资质（信息安全管理、信息系统审计、信息科技服务管理、网络、项目管理、数据库等专业领域高级资质）【3-4】分		
					4.风险管理职能部门中，信息科技风险管理专职人员均具有信息科技相关专业学历或工作经验，并且均获得获得信息科技高级专业资质（信息安全管理、信息系统审计、信息科技服务管理、网络、项目管理、数据库等专业领域高级资质）【4-5】分		
	信息科技风险管理策略（分值：20）	17	RM.03	信息科技风险管理纳入全面风险管理体系，信息科技风险管理制度（策略）覆盖组织及职能、制度规范、风险评估与风险监测等方面	1. 未设立信息科技风险管理部门（或组织），且未开展全面的信息科技风险评估活动【0-1】分	参考 T-B-2 第 1,2,3 项及附件	10
					2. 未设立信息科技风险管理部门（或组织），但信息科技部门定期或不定期开展全面的信息科技风险评估活动【1-2】分		
					3.信息科技风险管理部门隶属于信息科技部门，负责制定信息科技风险管理制度和流程，开展信息科技风险评估，风险评估结果经高管层审阅并向业务、风险管理、审计等部门传达【2-3】分		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					4.信息科技风险管理部门隶属于风险管理部门（合规、内控），负责制定信息科技风险管理制度和流程，开展信息科技风险评估，但风险评估结果仅在风险管理部门内部使用【3-4】分		
					5.信息科技风险管理部门隶属于风险管理部门（合规、内控），负责制定信息科技风险管理制度和流程，开展信息科技风险评估，风险评估结果经高管层审阅并向业务、信息科技、审计等部门传达【4-5】分		
		18	RM.04	定期评估信息科技风险管理制度的适用性、完整性并进行必要修订	1.未形成定期修订信息科技风险管理制度机制【0-3】分	参考 T-B-2 第 5 项	10
					2.形成定期修订信息科技风险管理制度机制【3-5】分		
	信息科技风险评估（分值：25）	19	RM.05	建立风险评估方法、流程、监测指标定期评审机制	1.未形成风险评估方法、流程、指标定期评审机制【0-3】分	参考 T-B-2 第 5 项	10
					2. 形成信息科技风险评估方法、流程、指标定期评审机制【3-5】分		
					扣分项： a) 组织开展信息科技风险评估的部门不是风险管理部门，扣【0.5】分； b) 未建立信息资产分类标准，扣【0.5】分； d) 未建立和维护信息资产清单，扣【0.5】分； e) 未对评估的风险制定风险处置计划或控制措施，扣【0.5】分。		
		20	RM.06	建立持续的信息科技风险监测机制，制定关键风险指标，并分配相关责任，持续进行风险监测，定期分析指标，监测信息科技风险发展趋势	1.未建立信息科技风险监测机制和信息科技风险监测关键指标【0-1】分	参考 T-B-2 第 4 项	15
					2.建立信息科技风险机制和信息科技风险监测关键风险点指标，但未对风险监测指标定期进行评审【1-3】分		
					3.建立信息科技风险机制和信息科技风险监测关键风险点指标，对风险监测指标定期进行评审，但风险监测结果未向各相关部门进行风险提示或未向高管层报告【3-4】分		
					4.建立信息科技风险机制和信息科技风险监测关键风险点指标，对风险监测指标定期进行评审，风险监测结果向各相关部门进行风险提示或向高管		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					层报告【4-5】分		
	信息安全意识培训（分值：15）	21	RM.07	定期组织在岗人员参加信息安全培训，并通过考核强化信息安全意识	根据本年度信息安全培训员工参与率： 1.【0-30%】，【0-1】分 2.【30%-60%】，【1-2】分 3.【60%-90%】，【2-3】分 4.【90%-100%】，【3-4】分 加分项：若机构建立了信息安全培训考核通过机制，可加【0.5-1】分	参考 T-B-2 第 6 项	15
审计（AD）权值：10%	信息科技内部审计独立性与合理授权（分值：20）	22	AD.01	内部审计部门报告路线合理性与独立性	1.先向高管层，再向董事会汇报，或仅向高管层汇报【0-1】分 2.同时向董事会或监事会，及高管层汇报【1-2】分 3.先向董事会或监事会，再向高管层汇报【2-3】分 4.直接向董事会或监事会汇报【3-5】分	参考 T-B-1 第 7 项	20
	信息科技专业内审人员（分值：30）	23	AD.02	信息科技审计部门通过任用具有信息科技审计专业资质的人才，实现信息科技审计专业化	1.内审部门中，未配备专职人员，或专职人员均无信息科技相关专业学历或工作经验【0-1】分 2.内审部门中，信息科技审计人员均具有信息科技相关专业学历或工作经验【1-3】分 3.内审部门中，信息科技审计人员均具有信息科技相关专业学历或工作经验，并且有一定数量人员获得信息科技高级专业资质（信息安全管理、信息系统审计、信息科技服务管理、网络、项目管理、数据库等专业领域高级资质）【3-4】分	参考 T-B-1 第 13 项	15

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					4.内审部门中，信息科技审计人员均具有信息科技相关专业学历或工作经验，并且均获得获得信息科技高级专业资质（信息安全管理、信息系统审计、信息科技服务管理、网络、项目管理、数据库等专业领域高级资质）【4-5】分		
	信息科技审计执行与问题整改情况（分值：50）	24	AD.03	信息科技内部审计覆盖情况	根据评估期内信息科技内部审计覆盖一级分支机构情况：	参考 T-B-3 第 2 项	20
					1.【0-30%】，【0-1】分		
					2.【30%-50%】，【1-2】分		
					3.【50%-70%】，【2-3】分		
					4.【70%-90%】，【3-4】分		
					5.【90%-100%】，【4-5】分		
		25	AD.04	信息科技内部审计整改情况	衡量范围包括评估期内开展的信息科技内部全面审计、专项审计以及综合性内部审计，以信息科技内部全面审计整改率为主要参考评估标准，以信息科技内部专项审计整改率作为重点辅助参考打分。专项审计和综合审计整改情况较好的，可将打分区间上浮一级。	参考 T-B-3 第 1 项	15
					1.【0-40%】，【0-2】分		
					2.【40%-60%】，【2-3】分		
					3.【60%-90%】，【3-4】分		
					4.【90%-100%】，【4-5】分		
		26	AD.05	信息科技外部审计整改情况	衡量范围包括评估期内开展的信息科技外部全面审计、专项审计以及综合性外部审计，以信息科技外部全面审计整改率为主要参考评估标准，以信息科技外部专项审计整改率作为重点辅助参考打分。专项审计和综合审计整改情况较好的，可将打分区间上浮一级。	参考 T-B-3 第 1 项	15
					1.【0-40%】，【0-2】分		
					2.【40%-60%】，【2-3】分		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					3.【60%-80%】，【3-4】分		
					4.【80%-100%】，【4-5】分		
系统开发及测试权值：10%)	系统开发项目管理（分值：20）	27	SD.01	建立专门的信息科技项目管理组织	根据建立专门的信息科技项目管理组织情况：	参考 T-B-4 第 2 项	10
					1.否，【0-1】分		
					2.是，但该组织未独立于项目开发团队【1-3】分		
					3.是，且该组织独立于项目开发团队【3-5】分		
		28	SD.02	设立业务需求管理组织，负责对业务需求进行整合和规范，发挥业务部门和开发部门联系的桥梁作用	根据机构已建立专门的需求管理组织情况：	参考 T-B-4 第 2 项	10
					1.否，【0-1】分		
					2.是，但未明确该组织的职能【1-3】分		
					2.是，且明确了该组织的职能【3-5】分		
	系统开发过程管理（分值：45）	29	SD.03	系统开发过程风险管理，有效识别信息科技项目风险，定期向项目管理组织沟通风险点、确定处置方案，并跟进处置方案的执行结果	以下 4 项得分之和为指标得分，第 5 项为加分项：	参考 T-B-4 第 2 项 参考 T-B-7 第 13 项	20
					1.项目计划里包括风险管理计划【0-1】分		
					2.在项目各阶段均进行风险评估【0-1】分		
					3.由专门的项目管理组织或风险管理组织来开展评估【0-1】分		
					4.将信息安全要求纳入系统设计【0-2】分		
					5.机构通过软件开发能力成熟度认证，CMM3 级及以上，CMMI2 级及以上，酌情增加【1-3】分		
		30	SD.04	设置独立于项目开发部门的质量保证人员，对项目过程质量进行监测、控制，有效控制项目质量，并定期向项目管理组织汇报	前 4 项得分之和减去第 5 项扣分项得分为指标得分：	参考 T-B-4 第 2 项	25
					1.质量保证人员项目参与率<100%【0-1】分；=100%，【0.5-1】分		
					2.项目代码安全检查完成率<100【0-1】分；=100%，【1-2】分		
					3.代码质量评审完成率<100%，【0-1】分；=100%，【0.5-1】分		
					4.通过质量管理体系认证并全面推广，【0.5-1】分		
					5.质量保证人员与开发（含测试）人员的职责分离情况，若职责分离情况		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					不佳扣【0-2】分		
	系统投产前准备（分值：25）	31	SD.05	系统变更、投产前，在生产验证环境中进行用户验收测试，及时发现并控制新系统上线风险	以下 7 项得分之和为指标得分： 1.本机构成立专门的测试管理组织【0-0.6】分 2.测试人员与开发人员独立【0-0.7】分 3.测试环境与开发环境独立【0-0.6】分 4.项目用户验收测试完成率=100%【0-0.6】分 5.项目压力测试完成率=100%【0-0.6】分 6.使用自动化测试和缺陷管理工具【0-0.5】分 7.测试人员与开发人员比例>50%【0-0.5】分	参考 T-B-4 第 1 项	25
信息科技运行（DS)权值：15%	事件管理（分值：25）	32	DS.01	由专门的部门或团队统一负责生产事件管理	以下 5 项得分之和为指标得分： 1.专门的部门（团队）统一管理各类生产事件【0-1】分 2.事先定义工作流程，实现事件生命周期管理（至少包括：事件的记录、分配、跟踪、反馈、考核、满意度调查等环节）【0-1】分 3.建立历史事件知识库【0-1】分 4.明确与变更管理的对接程序【0-1】分 5.明确与配置管理的对接程序【0-1】分	参考 T-B-7 第 13 项及附件	7
		33	DS.02	制定生产故障事件分级分类管理策略，通过合理的故障分级分类管理，按照不同级别和分类调用相应的资源处理，以实现快速、有效、有序地恢复系统和服务的	以下 4 项得分之和为指标得分： 1.按照事件性质建立生产事件分类，【0-1】分 2.基于严重性和影响程度建立生产故障事件优先级以及升级程序【0-1.5】分 3.建立历史事件知识库【0-1】分 4.定期开展运行维护团队培训【0-1.5】分	参考 T-B-7 第 13 项及附件	10

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
				正常运作			
		34	DS.03	运用统一的事件管理工具平台，监控异常、处理事件和投诉	以下 4 项得分之和为指标得分：	参考 T-B-7 第 13 项及附件	8
					1.在实际生产过程中借助软件工具实现生产故障事件管理【0-2】分		
					2.利用工具可实时采集生产环境中各类异常、故障、预警等信息【0-1】分		
					3.对于生产过程中的异常、故障、报警等信息，按照事件分类、分级管理标准反馈至对应的负责部门或人员进行处理【0-1】分		
					4.事件管理具有进度跟踪和质量考核功能【0-1】分		
	问题管理（分值：15）	35	DS.04	建立生产运行问题根源分析机制，通过制定问题解决方案，确保问题得到彻底解决，避免同类问题的重复发生	以下 3 项得分之和为指标得分：	参考 T-B-7 附件	15
					1.生产运行问题有完整记录，并具有相应的问题根源分析报告【0-1.5】分		
					2.生产运行问题根源分析报告内容规范，主要包含：问题种类、影响、紧急程度和优先级、问题的责任归属、问题根本原因、问题趋势分析、问题解决情况（已解决或未解决问题）、趋势分析等要素【0-1.5】分		
					3.问题解决情况经质量管理部门（或相关部门）共同确认，并主要由质量管理部门签发【0-2】分		
	可用性管理（分值：15）	36	DS.05	重要信息系统可用性	根据 4 个季度的核心业务系统可用率平均数：	参考全年 T-Q-1 第 2 项	5
					1.【98%-99%】，【0-2】分		
					2.【99%-99.5%】，【2-3】分		
					3.【99.5%-99.7%】，【3-4】分		
					4.【99.7%-100%】，【4-5】分		
		37	DS.06	制定合理的性能和容量管理监控报告机制，及时报告性能容量管理监测中发现	以下 3 项得分之和为指标得分：	参考 T-B-7 附件	10
					1.对于不同的重要信息系统分别定制有性能和容量监控指标和阈值【0-1】		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
				的问题，分析各项性能和容量指标是否超过阈值，并进行后续扩容、调优处理	分 2.定期监控和评估生产环境性能和容量，形成性能和容量评估报告【0-2】分 3.可以预警因性能和容量不足引起的生产事件，并按照已定义事件类别和等级进行处理【0-2】分		
	变更与维护（分值：25）	38	DS.07	授权变更率	计算公式：授权变更率=（授权生产变更数/生产变更总数）*100%： 1.【0-90%】，【0-1】分 2.【90%-95%】，【1-2】分 3.【95%-98%】，【2-4】分 4.【98%-100%】，【4-5】分	参考 T-B-7 第 12 项	8
		39	DS.08	控制生产环境系统变更实施过程风险	以下 4 项得分之和为指标得分： 1.以正式制度形式确定生产变更授权审批机制【0-1】分 2.所有涉及生产环境的变更，变更前制定回退和应急方案【0-1】分 3.利用工具自动记录所有变更，并实时存档和备份功能【0-1.5】分 4.内部审计人员或信息安全人员对生产变更记录定期审计核查【0-1.5】分	参考 T-B-7 第 13 项	8
		40	DS.09	生产变更管理	以下 5 项得分之和为指标得分： 1.建立完整的生产变更流程，包括：记录、评估、优先级排序、授权、结果审核、应急回退等【0-1】分 2.所有对业务有影响的生产变更由业务部门与科技部门共同签批后实施【0-1】分 3.针对紧急变更建立非常规流程，处理紧急变更的提出、测试、记录、评估和实施后授权【0-1】分	参考 T-B-7 第 13 项	9

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					4.常设生产变更应急团队，应对变更过程中的各类突发情况【0-1】分		
					5.常设生产变更验证团队，验证生产变更的正确性【0-1】分		
	系统运行操作（分值：20）	41	DS.10	具有规范的运行文档管理，配备准确的操作手册以指导运行人员操作	以下 5 项得分之和为指标得分：	参考 T-B-7 第 13 项	10
					1.建立运维文档生命周期管理流程【0-1】分		
					2.配置运行操作文档管理员岗位【0-1】分		
					3.运行操作文档经经验丰富的开发和运维人员共同审核后正式发布，运行操作文档成为运维人员培训的主要内容【0-1】分		
					4.建立文档变更流程保持运行操作文档与生产系统同步更新【0-1】分		
					5.重要信息系统与运行操作文档保持一对一关系【0-1】分		
		42	DS.11	运行人员进行生产系统操作时由独立人员对其操作步骤进行复核，减少出现操作失误的可能性	以下 3 项得分之和为指标得分：	参考 T-B-7 第 13 项	10
					1.运行人员进行生产系统操作时由独立人员对其操作步骤进行复核【0-1】分		
					2.信息安全部门或内审部门确定生产系统运行操作记录的保存范围、时限、内容，并定期审查【0-2】分		
					3.风险管理部门（合规、内控部门）确定的敏感岗位不存在兼职【0-2】分		
业务连续性（BC)权值：10%	灾难恢复体系建立与运作（分值：50）	43	BC.01	建立灾难恢复的关键基础设施	1、未建立应对灾难的同城实时或定期数据备份【0】分	参考 T-B-10 第 3,4 项 参考 T-B-12 相	15
					2、已建立应对灾难的同城实时或定期数据备份，并可至少保障核心、柜面业务恢复【0-1】分		
					3、已建立应对灾难的异地实时或定期数据备份，并可至少保障核心、柜面业务恢复【1-2】分		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					4、已建立同城灾备中心（灾备机房），至少可保障核心、柜面业务应用级备份，并按以下要点单选得分： （1）一主一备：一个生产中心对应一个备份中心【2-3】分 （2）一主多备：一个生产中心对应多个备份中心【2.5-3.5】分 （3）多主多备：多个生产中心对应多个备份中心【2.5-3.5】分 （4）多主一备：多个生产中心共享一个备份中心【2-3】分 （5）互为备份：多个生产中心互相备份【3-3.5】分	关项	
					5、已建立异地灾备中心（灾备机房），至少可保障核心、柜面业务应用级备份，并按以下要点单选得分： （1）一主一备：一个生产中心对应一个备份中心【3-4】分 （2）一主多备：一个生产中心对应多个备份中心【3.5-4.5】分 （3）多主多备：多个生产中心对应多个备份中心【3.5-4.5】分 （4）多主一备：多个生产中心共享一个备份中心【3-4】分 （5）互为备份：多个生产中心互相备份【4-5】分		
		44	BC.02	灾难恢复体系得到必要的技术和管理措施支撑运作	以下 6 项得分之和为指标得分：	参考 T-B-12 相关项	15
					1、以文件或制度形式明确了灾难恢复计划启动条件【0-0.9】分		
					2、灾难恢复计划（DRP）文件由高管层签发【0-0.8】分		
					3、灾难恢复计划定期修订【0-0.8】分		
					4、定期开展业务影响分析【0-0.8】分		
					5、成立来自风险、业务、后勤、信息技术等部门组成的灾难恢复技术支持团队，并定期开展灾备切换演练【0-0.8】分		
					6、已建立核心业务系统的生产环境和灾备环境同步机制，并定期核对【0-0.9】分		
		45	BC.03	通过业务影响分析，定义重	1、未确定灾难恢复目标(RTO,RPO)，【0】分	参考	10

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
				要信息系统的 RTO/RPO	2、未经业务影响分析，但确定了重要信息系统的 RTO/RPO,【1-2】分	T-B-12 附件	
					3、经业务影响分析后，确定重要信息系统 RTO/RPO,【2-5】分		
					4、重要信息系统 RTO 最大值超过 4 小时,RPO 最大值超过 30 分钟,减【1-2】分		
		46	BC.04	重要信息系统灾备覆盖率		参考 T-B-7、T-B-12 附件	10
					1、【0-60%】，【0-3】分		
					2、【60%-80%】或者核心、柜面、银行卡系统已纳入灾备，【3-4】分		
					3、【80%-100%】，其中包含核心、柜面、银行卡系统，【4-5】分		
	应急管理体系建立及运作（分值：50）	47	BC.05	设立重要信息系统重大突发事件应急组织	1、未设立重大突发事件应急组织【0-1】分	参考 T-B-11 第 1 项	16
					2、总行层面设立重大突发事件应急组织，但成员仅为信息科技部门人员【1-2】分		
					3、总行层面设立重大突发事件应急组织，并纳入全行应急管理体系，成员包含高管层、业务、财务、行政后勤等部门人员【2-4】分		
					4、总行层面设立重大突发事件应急组织，并纳入全行应急管理体系，成员包含高管层、业务、财务、行政后勤等部门人员，一级分支机构亦成立相应应急组织【4-5】分		
		48	BC.06	已签定服务水平协议或建立应急沟通机制的第三方范围	以下 8 项得分之和为指标得分：	参考 T-B-12 相关项	16
					1、电力【0-0.7】分		
					2、电信运营商【0-0.6】分		
					3、公安部门【0-0.7】分		
					4、银联【0-0.6】分		
					5、国际卡组织【0-0.6】分		
					6、反钓鱼联盟（组织）【0-0.6】分		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					7、软件服务商服务水平协议签订率=100%【0-0.6】分		
					8、硬件服务商服务水平协议签订率=100%【0-0.6】分		
		49	BC.07	重要信息系统应急演练覆盖率	计算公式：重要信息系统应急演练覆盖率=（本年度应急演练覆盖的重要信息系统数）/（重要信息系统总数）*100%	参考 T-B-7、T-B-12 附件	18
					1、【0-80%】，【0-3】分		
					2、【80%-90%】，【3-4】分		
					3、【90%-100%】，【4-5】分		
信息科技外包（OS）权值：10%	评估外包风险（分值：20）	50	OS.01	建立信息科技外包风险评估机制	以下 4 项得分之和为指标得分：	参考 T-B-16 第 2 项	10
					1.风险管理部门统一制定评估方法和工作流程，包括信息科技外包风险方法和工作流程【0-1】分		
					2.质量管理团队设计确定信息科技外包服务质量考核指标【0-1】分		
					3.信息科技外包项目立项阶段风险评估率为 100%【0-1】分		
					4.项目实施过程中定期开展风险评估【0-2】分		
		51	OS.02	建立应对外包商失效、异常退出应急方案	1.未制定外包商异常退出应急预案【0-1】分	参考 T-B-16 第 2 项	10
					2.制定外包商异常退出应急预案，但未开展演练【1-3】分		
					3.制定外包商异常退出应急预案，并演练成功【3-5】分		
	外包人员管理（分值：30）	52	OS.03	控制外包人员自带设备或软件工具执行开发任务，防范外包人员使用非授权软件、设备，避免外包人员危及机构信息资产安全	以下 4 项得分之和为指标得分：	参考 T-B-16 第 2 项	30
					1.与外包商签署专门的保密协议【0-1】分		
					2.严禁外包人员自带设备或软件工具访问机构网络，外包人员所使用的设备中安装由安全监测工具，可记录外包人员的操作过程【0-1.5】分		
					3.严禁外包人员直接操作生产系统【0-1.5】分		
					4.与外包人员签定个人保密承诺书【0-1】分		
	合同管	53	OS.04	制定完善的外包合同框架，	以下 4 项得分之和为指标得分：	参考	15

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
	理（分值：15）			包含知识产权、服务水平、保密协议、保留审计权力、应急响应要求、损失赔偿、培训和知识转移、外包安排变更和终止等关键要素，防范合同内容缺失导致的法律风险	1.外包合同模板经法律部门统一编制【0-2】分 2.外包合同签订前经内审部门审核【0-1】分 3.外包合同签订前经法律部门审核【0-1】分 4.外包合同具有保留审计和监管部门延伸检查权力的条款【0-1】分	T-B-16 第 2 项	
	服务交付与监督（分值：35）	54	OS.05	监督衡量外包服务交付质量	视外包商服务水平达标率打分 1.【0-60%】，【0-1】分 2.【60%-70%】，【1-2】分 3.【70%-80%】，【2-3】分 4.【80%-90%】，【3-4】分 5.【90%-100%】，【4-5】分	参考 T-B-16 第 2 项	10
		55	OS.06	降低对外包商的过度依赖	以下 3 项得分之和为指标得分： 1.核心业务系统为自主研发，源码知识产权为机构所有【0-2】分 2.网上银行系统为自主研发，源码知识产权为机构所有【0-1.5】分 3.安全、保密设备（系统）由机构自主运维【0-1.5】分	参考 T-B-16 第 1 项	10
信息安全（GC）权值：18%	物理安全（分值：15）	56	GC.01	全面的数据中心（中心机房）物理环境控制，通过有效的环境控制防控可能造成计算机设备硬件故障或损坏的风险	以下 7 项得分之和为指标得分： 1.中心机房按照功能、重要性级别划分物理安全区域【0-1】分 2.专门的部门或团队负责物理环境和硬件设备的统一管理【0-0.5】分 3.门禁系统为国产设备【0-0.5】分 4.门禁系统采用双重认证方式【0-0.5】分 5.动力环境监控预警范围至少覆盖：机房环境、安防监控、消防、防水、	参考 T-B-6 相关项目	6

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					防静电、防鼠、UPS、供配电、防雷等要素【0-1】分		
					6.明确监控记录保存期限【0-0.5】分		
					7.同时采取短信、声音、光学等多种有效方式报警【0-1】分		
		57	GC.02	形成定期巡检物理环境制度，及时发现隐患和故障，保障设备运行的连续性	以下 4 项得分之和为指标得分：	参考 T-B-6 相关项目	9
					1.制定机房定期全面巡检制度【0-1】分		
					2.每天执行 1 次以上全面机房巡检【0-1】分		
					3.机房巡检记录保存期限符合审计或风险管理部门要求【0-1】分		
					4.信息安全团队或人员定期或不定期检查机房巡检制度执行情况【0-2】分		
	物理访问控制（分值：10）	58	GC.03	门禁记录保存期限满足安全检查需求	根据各中心机房门禁记录保存时间的最小值（短板原则）：	参考 T-B-6 相关项目	5
					1.1 个月以下【0-1】分。		
					2.1-3 个月【1-2】分		
					3.3-6 个月【2-3】分		
					4.半年至 1 年【3-4】分		
					5.1 年以上【4-5】分		
		59	GC.04	环境监控记录保存期限足够长	根据各中心机房监控记录保存时间的最小值（短板原则）：	参考 T-B-6 相关项目	5
					1.3 个月以下【0-1】分。		
					2.3-6 个月【1-2】分		
					3.半年至 1 年【2-3】分		
					4.1 年至 2 年【3-4】分		
					5.2 年以上【4-5】分		
	逻辑访	60	GC.05	建立重要信息系统访问控	以下 4 项得分之和为指标得分：	参考 T-B-7	15

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
	问控制（分值：15）			制策略技术规范	1.信息安全团队或信息科技风险管理部门统一制定重要信息系统逻辑访问控制策略和技术规范【0-1.5】分	相关项目、附件	
					2.采取密码管理工具强制执行密码安全策略，至少包括口令复杂度、更新周期、保留访问日志等【0-1】分		
					3.建立重要信息系统用户权限生命周期管理规范，包括用户权限的新建、变更、禁用、删除等策略【0-1】分		
					4.信息安全团队、内审人员或信息科技风险管理部门定期复查和审核逻辑访问控制策略的执行情况【0-1.5】分		
	配置管理（分值：10）	61	GC.06	建立生产环境配置管理策略	以下 4 项得分之和为指标得分：	参考 T-B-7 相关项目、附件	10
					1.建立生产环境配置管理数据库【0-1】分		
					2.运用配置管理工具进行管理【0-1】分		
					3.定期复核配置管理项的准确性和一致性【0-1.5】分		
					4.配置管理数据库备份介质同城或异地存放【0-1.5】分		
	网络管理（分值：15）	62	GC.07	建立定期分析和审查信息安全事件制度	以下 3 项得分之和为指标得分：	参考 T-B-9 相关项目、附件	3
					1.明确网络安全设备的维护和管理职责【0-1】分		
					2.指定专职人员检查信息安全事件【0-2】分		
					3.建立信息安全事件升级程序【0-2】分		
		63	GC.08	网上银行边界有效防护	以下 8 项得分之和为指标得分：	参考 T-B-9 第 2 项	3
					1.异构防火墙【0-0.6】分		
					2.热备防火墙【0-0.6】分		
					3.入侵检测系统（IDS）【0-0.6】分		
					4.入侵防御系统（IPS）【0-0.6】分		
					5.与电信运营商签订 DDoS 清洗服务【0-0.8】分		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
					6.访问列表（ACL）【0-0.6】分		
					7.防病毒网关【0-0.6】分		
					8.蜜罐技术【0-0.6】分		
		64	GC.09	生产网与其他网络的有效隔离	根据生产网与其他网络隔离情况：	参考 T-B-9 第 5 项	3
					1.物理隔离及逻辑隔离：未覆盖开发网、测试网、办公网、互联网【0-1】分		
					2.物理隔离及逻辑隔离：覆盖开发网、测试网、办公网、互联网【1-2】分		
					3.物理隔离：开发网、测试网，逻辑隔离:办公网、互联网【2-3】分		
					4.物理隔离：开发网、测试网、办公网，逻辑隔离:互联网【3-4】分		
					5.物理隔离：开发网、测试网、办公网、互联网【4-5】分		
		65	GC.10	所有 Windows 设备都安装防病毒软件	根据防病毒软件安装覆盖率：	参考 T-B-9 第 9 项	3
					1.【0-95%】，【0-2】分		
					2.【95%-98.5%】，【2-3】分		
					3.【98.5%-99.5%】，【3-4】分		
					4.【99.5%-100%】，【4-5】分		
		66	GC.11	及时更新防病毒软件特征码	根据病毒特征码更新率：	参考 T-B-9 第 9 项	3
					1.【0-95%】，【0-2】分		
					2.【95%-98.5%】，【2-3】分		
					3.【98.5%-99.5%】，【3-4】分		
					4.【99.5%-100%】，【4-5】分		
	数据管理与保	67	GC.12	建立数据备份与恢复策略	以下 4 项得分之和为指标得分：	参考 T-B-10 第 1	5
					1.建立专门数据管理组织【0-1】分		

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
	护（分值：20）				2. 书面定义的数据管理制度【0-1】分	项	
					3. 根据数据性质、重要程度，定义的数据重要性或敏感性标准【0-2】分		
					4. 根据分类分级标准制定数据备份与恢复策略【0-1】分		
		68	GC.13	在安全的环境中保存数据存储介质	以下 7 项得分之和为指标得分：	参考 T-B-10 第 4 项	5
					1、防火【0-0.7】分		
					2、防水【0-0.7】分		
					3、防磁【0-0.8】分		
					4、防盗【0-0.7】分		
					5、防鼠【0-0.7】分		
					6、温湿度控制【0-0.7】分		
					7、抗震【0-0.7】分		
		69	GC.14	安全清除重要数据介质、设备当中的敏感数据	以下 3 项得分之和为指标得分：	参考 T-B-10 第 6 项	5
					1. 对已失效数据或已毁坏但包含重要数据的介质消磁、物理粉碎等【0-1.5】分		
					2. 重要数据介质交由国家保密安全部门指定或认证的销毁机构处理【0-1.5】分		
					3. 信息安全团队或信息科技风险管理部门定期或不定期核查重要数据介质销毁制度执行情况【0-2】分		
		70	GC.15	严格限制移动设备在生产环境中的使用	以下 3 项得分之和为指标得分：	参考 T-B-10 第 5 项	5
					1. 建立移动存储设备在生产环境中的使用管理制定【0-2】分		
					2. 生产环境中使用专用且经加密处理的移动设备【0-2】分		
					3. 采用技术或管理措施监控移动设备访问生产环境过程【0-1】分		
	网上银	71	GC.16	定期开展网上银行（含网上	根据网上银行渗透性测试开展情况：	参考	5

子领域	关键控制目标	序号	编码	指标	参考评估标准（最高分不得超过 5 分）	数据来源	指标分值
	行安全（分值：15）			商城等）渗透性测试	1.评估期内未开展网上银行渗透性测试，【0】分	T-B-14 第 5 项及附件	
					2. 评估期内开展网上银行渗透性测试，视测试覆盖范围，测试效果【1-3】分		
					3. 已建立定期开展网上银行渗透性测试的机制，并连续两年以上开展渗透性测试工作【3-5】分		
		72	GC.17	网上银行客户安全	以下 4 项得分之和为指标得分：	参考 T-B-14 第 5 项及附件	5
					1.客户端程序经过代码安全检测【0-1】分		
					2.强制双因素身份验证【0-2】分		
					3.客户端程序采取反汇编分析措施【0-1】分		
					4.开办网上银行业务时，向客户明确提示风险和注意事项【0-1】分		
		73	GC.18	防范网上银行外部攻击及欺诈	根据网上银行钓鱼网站（IP 地址）关闭率：	参考 T-B-14 第 5 项	5
					1.【0-50%】，【0-2】分		
					2.【50%-80%】，【2-3】分		
					3.【80%-95%】，【2-4】分		
					4.【95%-100%】，【4-5】分		

附件三 综合评估结论描述参考

	一级	二级	三级	四级	五级	六级
信息科技风险	表示对于机构固有风险水平，控制措施相对健全。因此，剩余的信息科技风险水平为一级，几乎不可能对信息科技目标实现造成影响	表示对于机构固有风险水平，控制措施虽然存在一定不足，但相对完整，能够与固有风险水平相适应。因此，剩余的信息科技风险水平为二级，不太可能会对信息科技目标实现造成重大影响	表示对于机构固有风险水平，控制措施虽然存在某些不足，但仍基本与固有风险水平相适应。因此，剩余的信息科技风险水平为三级，可能会对信息科技目标实现造成有限影响	表示对于机构固有风险水平，控制措施存在某些不足，难以与固有风险水平相适应。因此，剩余的信息科技风险水平为四级，有可能对信息科技目标实现造成重大影响，从而影响机构业务正常运行和经营目标的实现。应该给予一定的监管关注	表示对于机构固有风险水平，控制措施存在重大不足，几乎不能与固有风险水平相适应。因此，剩余的信息科技风险水平五级，很可能对信息科技目标实现造成重大影响，从而影响机构业务正常运营。需要给予监管关注以及一个明确的限期整改计划	表示对于机构固有风险水平，控制措施存在重大缺陷，不能与固有风险水平相适应。因此，剩余的信息科技风险水平六级，很可能对信息科技目标实现造成重大影响，从而影响机构业务正常运营，甚至引发公众对其金融服务质量的质疑。需要给予密切的监管关注以及一个明确的限期整改计划
监管意见	在确定机构提供信息的真实性的前提下，应积极支持其信息科技发展，一般不需要特别的监管行动和措施，可以在现场检查的频率上相应放宽	在确定机构提供信息的真实性的前提下，需要指出其信息科技方面存在的薄弱环节，由机构自行斟酌改进，可以在现场检查的频率上相应放宽	在确定机构提供信息的真实性的前提下，需要指出其信息科技方面存在的薄弱环节，督促其做出相应的整改，现场检查时应重点关注其存在的风险	需要适当加强对其非现场监管分析与现场检查的频度和深度，督促其加强信息科技风险管理，改善信息科技状况	应提高现场检查频率，加大现场检查力度，密切关注其信息科技状况，督促其加大信息科技调整力度，积极降低风险，必要时应对其高级管理人员进行谈话，责令整改	应提高现场检查频率，加大现场检查力度，密切关注其信息科技状况，督促其加大信息科技调整力度，积极降低风险，同时在机构准入和新业务系统投产、新设信息科技项目、信息系统重大变更等方面进行严格限制，必要时应对其高级管理人员进行谈话，责令整改