电子银行安全评估指引

中国银行业监督管理委员会关于印发《电子银行安全评估指引》的通知

（银监发〔2006〕9号）

各银监局，各国有商业银行、股份制商业银行：

现将《电子银行安全评估指引》印发给你们，请参照执行。请各银监局将此件转发辖内有关金融机构。

二〇〇六年一月二十六日

电子银行安全评估指引

（2006年1月26日）

第一章　总　则

第一条　为加强电子银行业务的安全与风险管理，保证电子银行安全评估的客观性、及时性、全面性和有效性，依据《电子银行业务管理办法》的有关规定，制定本指引。

第二条　电子银行的安全评估，是指金融机构在开展电子银行业务过程中，对电子银行的安全策略、内控制度、风险管理、系统安全、客户保护等方面进行的安全测试和管控能力的考察与评价。

第三条 开展电子银行业务的金融机构，应根据其电子银行发展和管理的需要，至少每 2 年对电子银行进行一次全面的安全评估。

第四条 金融机构可以利用外部专业化的评估机构对电子银行进行安全评估，也可以利用内部独立于电子银行业务运营和管理部门的评估部门对电子银行进行安全评估。

第五条 金融机构应建立电子银行安全评估的规章制度体系和工作规程，保证电子银行安全评估能够及时、客观地得以实施。

第六条 金融机构的电子银行安全评估，应接受中国银行业监督管理委员会（以下简称中国银监会）的监督指导。

第二章 安全评估机构

第七条 承担金融机构电子银行安全评估工作的机构，可以是金融机构外部的社会专业化机构，也可以是金融机构内部具备相应条件的相对独立部门。

第八条 外部机构从事电子银行安全评估，应具备以下条件：

（一） 具有较为完善的开展电子银行安全评估业务的管理制度和操作规程；

（二） 制定了系统、全面的评估手册或评估指导文件，评估手册或评估指导文件的内容应至少包括评估程序、评估

方法和依据、评估标准等；

（三） 拥有与电子银行安全评估相关的各类专业人才，了解国际和中国相关行业的行业标准；

（四） 中国银监会规定的其他从事电子银行安全评估应当具备的条件。

第九条 金融机构内部部门从事电子银行安全评估，除应具备第八条 规定的有关条件外，还应具备以下条件：

（一） 必须独立于电子银行业务系统开发部门、运营部门和管理部门；

（二） 未直接参与过有关电子银行设备的选购工作。

第十条 中国银监会负责电子银行安全评估机构资质认定工作。

电子银行安全评估机构在开展金融机构电子银行安全评估业务前，可以向中国银监会申请对其资质进行认定。

第十一条 金融机构在进行电子银行安全评估时，可以选择经中国银监会资质认定的安全评估机构，也可以选择未经中国银监会资质认定的安全评估机构。

金融机构选择经中国银监会资质认定的安全评估机构时，有关安全评估机构的管理适用本指引有关规定。金融机构选择未经中国银监会资质认定的安全评估机构时，安全评估机构的选择标准应不低于第八条、第九条规定的条件要

求，并应按照《电子银行业务管理办法》的有关规定，报送相关材料。

电子银行安全评估机构无论是否经过中国银监会资质认定，在开展电子银行安全评估活动时，都应遵守有关电子银行安全评估实施和管理的规定。

第十二条 中国银监会每年将组织一次电子银行安全评估机构资质认定工作，评定时间应提前 1 个月公告。

第十三条 申请资质认定的电子银行安全评估机构，应在中国银监会公告规定的时限内提交以下材料（一式七份）：

（一） 电子银行安全评估资质认定申请报告；

（二） 机构介绍；

（三） 安全评估业务管理框架、管理制度、操作规程等；

（四） 评估手册或评估指导文件；

（五） 主要评估人员简历；

（六） 中国银监会要求提供的其他文件、资料。

第十四条 中国银监会收到安全评估机构资质认定申请完整材料后，组织有关专家和监管人员对申请材料进行评议，采用投票的办法评定电子银行安全评估机构是否达到了有关资质要求。

第十五条 中国银监会对评估机构资质评议后，出具《电子银行安全评估机构资质认定意见书》，载明评议意见，对评估机构的资质做出认定。

第十六条 中国银监会出具的《电子银行安全评估机构资质认定意见书》，仅供评估机构与金融机构商恰有关电子银行安全评估业务时使用，不影响评估机构开展其他经营活动。

评估机构不得将《电子银行安全评估机构资质认定意见书》用于宣传或其他活动。

第十七条 经中国银监会评议并被认为达到有关资质要求的评估机构，每次资质认定的有效期限为2年。

经评议不符合认定资质的，评估机构可在下一年度重新申请资质认定。

第十八条 在资质认定的有效期限内，电子银行安全评估机构如果出现下列情况，中国银监会将撤销已做出的评议和认定意见：

（一） 评估机构管理不善，其工作人员泄露被评估机构秘密的；

（二） 评估工作质量低下，评估活动出现重要遗漏的；

（三） 未按要求提交评估报告，或评估报告中存在不实表述的；

（四） 将《电子银行安全评估机构资质认定意见书》用于宣传和其他经营活动的；

（五） 存在其他严重不尽职行为的。

第十九条 评估机构有下列行为之一的，中国银监会将在一定期限或无限期不再受理评估机构的资质认定申请，金融机构不应再委托该评估机构进行安全评估：

（一） 与委托机构合谋，共同隐瞒在安全评估过程中发现的安全漏洞，未按要求写入评估报告的；

（二） 在评估过程中弄虚作假，编造安全评估报告的；

（三） 泄漏被评估机构机密信息，或不当使用被评估机构机密资料的。

金融机构内部评估机构出现以上情况之一的，中国银监会将依法对相关机构和责任人进行处罚。

第二十条 中国银监会认可的电子银行安全评估机构，以及有关资质认定、撤销等信息，仅向开展电子银行业务的各金融机构通报，不向社会发布。

金融机构不得向第三方泄露中国银监会的有关通报信息，影响有关机构的其他业务活动，也不得将有关信息用于与电子银行安全评估活动无关的其他业务活动。

第二十一条 金融机构可以在中国银监会认定的评估机构范围内，自主选择电子银行安全评估机构。

第二十二条 电子银行主要系统设置于境外并在境外实施电子银行安全评估的外资金融机构，以及需要按照所在地监管部门的要求在境外实施电子银行安全评估的中资金融机构境外分支机构，电子银行安全评估机构的选择应遵循所在国家或地区的法律要求。

所在国家或地区没有相关法律要求的，金融机构应参照本指引的有关规定开展安全评估活动。

第二十三条 金融机构应与聘用的电子银行安全评估机构签订书面服务协议，在服务协议中，必须含有明确的保密条款和保密责任。

金融机构选择内部部门作为评估机构时，应由电子银行管理部门与评估部门签订评估责任确定书。

第二十四条 安全评估机构应根据评估协议的规定，认真履行评估职责，真实评估被评估机构电子银行安全状况。

第三章 安全评估的实施

第二十五条 评估机构在开始电子银行安全评估之前，应就评估的范围、重点、时间与要求等问题，与被评估机构进行充分的沟通，制定评估计划，由双方签字认可。

第二十六条 依据评估计划，评估机构进场对委托机构的电子银行安全进行评估。

电子银行安全评估应真实、全面地评价电子银行系统的安全性。

第二十七条 电子银行安全评估至少应包括以下内容：

（一） 安全策略；

（二） 内控制度建设；

（三） 风险管理状况；

（四） 系统安全性；

（五） 电子银行业务运行连续性计划；

（六） 电子银行业务运行应急计划；

（七） 电子银行风险预警体系；

（八） 其他重要安全环节和机制的管理。

第二十八条 电子银行安全策略的评估，至少应包括以下内容：

（一） 安全策略制定的流程与合理性；

（二） 系统设计与开发的安全策略；

（三） 系统测试与验收的安全策略；

（四） 系统运行与维护的安全策略；

（五） 系统备份与应急的安全策略；

（六） 客户信息安全策略。

评估机构对金融机构安全策略的评估，不仅要评估安全策略、规章制度和程序是否存在，还要评估这些制度是否得

到贯彻执行，是否及时更新，是否全面覆盖电子银行业务系统。

第二十九条 电子银行内控制度的评估，应至少包括以下内容：

（一） 内部控制体系总体建设的科学性与适宜性；

（二） 董事会和高级管理层在电子银行安全和风险管理体系中的职责，以及相关部门职责和责任的合理性；

（三） 安全监控机制的建设与运行情况；

（四） 内部审计制度的建设与运行情况。

第三十条 电子银行风险管理状况的评估，应至少包括以下内容：

（一） 电子银行风险管理架构的适应性和合理性；

（二） 董事会和高级管理层对电子银行安全与风险管理的认知能力与相关政策、策略的制定执行情况；

（三） 电子银行管理机构职责设置的合理性及对相关风险的管控能力；

（四） 管理人员配备与培训情况；

（五） 电子银行风险管理的规章制度与操作规定、程序等的执行情况；

（六） 电子银行业务的主要风险及管理状况；

（七） 业务外包管理制度建设与管理状况。

第三十一条 电子银行系统安全性的评估，应至少包括以下内容：

（一） 物理安全；

（二） 数据通讯安全；

（三） 应用系统安全；

（四） 密钥管理；

（五） 客户信息认证与保密；

（六） 入侵监测机制和报告反应机制。

评估机构应突出对数据通讯安全和应用系统安全的评估，客观评价金融机构是否采用了合适的加密技术、合理设计和配置了服务器和防火墙，银行内部运作系统和数据库是否安全等，以及金融机构是否制定了控制和管理修改电子银行系统的制度和控制程序，并能保证各种修改得到及时测试和审核。

第三十二条 电子银行业务运行连续性计划的评估，应至少包括以下内容：

（一） 保障业务连续运营的设备和系统能力；

（二） 保证业务连续运营的制度安排和执行情况。

第三十三条 电子银行业务运行应急计划的评估，应至少包括以下内容：

（一） 电子银行应急制度建设与执行情况；

（二） 电子银行应急设施设备配备情况；

（三） 定期、持续性检测与演练情况；

（四） 应对意外事故或外部攻击的能力。

第三十四条 评估机构应制定本机构电子银行安全评定标准，在进行安全评估时，应根据委托机构的实际情况，确定不同评估内容对电子银行总体风险影响程度的权重，对每项评估内容进行评分，综合计算出被评估机构电子银行的风险等级。

第三十五条 评估完成后，评估机构应及时撰写评估报告，并于评估完成后 1 个月内向委托机构提交由其法定代表人或其授权委托人签字认可的评估报告。

第三十六条 评估报告应至少包括以下内容：

（一） 评估的时间、范围及其他协议中重要的约定；

（二） 评估的总体框架、程序、主要方法及主要评估人员介绍；

（三） 不同评估内容风险权重的确定标准，风险等级的计算方法，以及风险等级的定义；

（四） 评估内容与评估活动描述；

（五） 评估结论；

（六） 对被评估机构电子银行安全管理的建议；

（七） 其他需要说明的问题；

（八） 主要术语定义和所采用的国际或国内标准介绍

（可作为附件）；

（九） 评估工作流程记录表（可作为附件）；

（十） 评估机构参加评估人员名单（可作为附件）。

在评估结论中，评估机构应采用量化的办法表明被评估机构电子银行的风险等级，说明被评估机构电子银行安全管理中存在的主要问题与隐患，并提出整改建议。

第三十七条 评估报告完成并提交委托机构后，如需修改，应将修改的原因、依据和修改意见作为附件附在原报告之后，不得直接修改原报告。

第四章 安全评估活动的管理

第三十八条 金融机构在申请开办电子银行业务时，应当按照有关规定对完成测试的电子银行系统进行安全评估。

第三十九条 金融机构开办电子银行业务后，有下列情形之一的，应立即组织安全评估：

（一） 由于安全漏洞导致系统被攻击瘫痪，修复运行的；

（二） 电子银行系统进行重大更新或升级后，出现系统意外停机 12 小时以上的；

（三） 电子银行关键设备与设施更换后，出现重大事故修复后仍不能保持连续不间断运行的；

（四） 基于电子银行安全管理需要立即评估的。

第四十条 金融机构对电子银行外部安全评估机构的选聘，应由金融机构的董事会或高级管理层负责。

第四十一条 已实现数据集中管理的银行业金融机构，其分支机构开展电子银行业务不需单独进行安全评估，在总行（公司）的电子银行安全评估中应包含对其分支机构电子银行安全管理状况的评估。

第四十二条 未实现数据集中管理的银行业金融机构，其分支机构开展电子银行业务且拥有独立的业务处理设备与系统的，分支机构的电子银行系统应在总行（公司）的统一管理和指导下，按照有关规定进行安全评估。

第四十三条 电子银行主要业务处理系统设置在境外的外资金融机构，其境外总行（公司）已经进行了安全评估且符合本指引有关规定的，其境内分支机构开展电子银行业务不需单独进行安全评估，但应按照本指引的有关要求，向监管部门报送安全评估报告。

第四十四条 电子银行主要业务处理系统设置在境内的外资金融机构，或者虽设置在境外但其境外总行（公司）未进行安全评估或安全评估不符合本指引有关规定的，应按规定开展电子银行安全评估工作。

第四十五条 电子银行安全评估工作，确需由多个评估机构共同承担或实施时，金融机构应确定一个主要的评估机

构协调总体评估工作，负责总体评估报告的编制。

金融机构将电子银行系统委托给不同的评估机构进行安全评估，应当明确每个评估机构安全评估的范围，并保证全面覆盖了应评估的事项，没有遗漏。

第四十六条 金融机构应在签署评估协议后两周内，将评估机构简介、拟采用的评估方案和评估步骤等，报送中国银监会。

第四十七条 中国银监会根据监管工作的需要，可派员参加金融机构电子银行安全评估工作，但不作为正式评估人员，不提供评估意见。

第四十八条 评估机构应本着客观、公正、真实和自主的原则，开展评估活动，并严格保守在评估过程中获悉的商业机密。

第四十九条 在评估过程中，委托机构和评估机构之间应建立信息保密工作机制：

（一） 评估过程中，调阅相关资料、复制相关文件或数据等，都应建立登记、签字制度；

（二） 调阅的文件资料应在指定的场所阅读，不得带出指定场所；

（三） 复制的文件或数据一般也不应带出工作场所，如确需带出的，必须详细登记带出文件或数据名称、数量、带

出原因、文件与数据的最终处理方式、责任人等，并由相关负责人签字确认；

（四） 评估过程中废弃的文件、材料和不再使用的数据，应立即予以销毁或删除；

（五） 评估工作结束后，双方应就有关机密数据、资料等的交接情况签署说明。

第五十条 金融机构在收到评估机构评估报告的 1 个月内，应将评估报告报送中国银监会。

金融机构报送评估报告时，可对评估报告中的有关问题作必要的说明。

第五十一条 未经监管部门批准，电子银行安全评估报告不得作为广告宣传资料使用，也不得提供给除监管部门以外的第三方机构。

第五十二条 对未按有关要求进行的安全评估，或者评估程序、方法和评估报告存在重要缺陷的安全评估，中国银监会可以要求金融机构进行重新评估。

第五十三条 中国银监会根据监管工作的需要，可以自己组织或委托评估机构对金融机构的电子银行系统进行安全评估，金融机构应予以配合。

第五十四条 中国银监会根据监管工作的需要，可直接向评估机构了解其评估的方法、范围和程序等。

第五十五条 对于评估报告中所反映出的问题，金融机构应采取有效的措施加以纠正。

第五章 附则

第五十六条 本指引由中国银监会负责解释。

第五十七条 本指引自2006年3月1日起施行。