电子银行和电子货币交易的风险管理

(巴塞尔委员会 1998 年 3 月通过)

李宪普 李宪明 王佳 翻译^①

1. 引言

在电子商务的发展中，电子支付手段将会是举足轻重的，包括电子货币在内的零售电子银行服务和产品，能为银行带来非同小可的新机遇。电子银行可以使银行为传统的存款、放贷活动拓展市场，并在提供现有的支付服务时提供新的产品、服务或加强其竞争地位。此外，电子银行可以减少银行的经营成本。

广而言之，电子银行及电子货币不断的发展，将有助于提高银行业和支付系统的效率，以及降低国内和国际零售交易成本。其潜在影响是，提高生产率，增进经济福利。利用电子银行和电子货币支付和收款，消费者和商人也可提高效率，并享受到更大的便利。电子银行也可以增加消费者利用金融系统的机会，而在过去，他们使用金融系统的渠道是有限的。

对本报告的研究范围有必要从两方面进行限制。首先，报告仅从银行监管的角度研究了电子银行和电子货币交易的风险管理，而未涉及诸如金融后果之类的问题。其二，报告中提及的许多风险同时适用于银行及非银行的发行人和供应者，但报告仅阐述有关银行的情况。

1.1 目的和组织

电子货币和一些电子银行的发展与应用仍然处于初级阶段。考虑到将来技术和市场发展的不确定性，监管机构避免采取哪些阻碍有益的革新和实验的政策，是很重要的。同时，基本委员会认识到，电子银行和电子货币交易给银行业带来利润的同时，也带来风险，因此必须平衡这些风险与利润。

本文的目的是，为监管机构和银行组织提供一些思路，从而有助于他们开发有关识别、评估、管理和控制与电子银行和电子货币相关的风险的方法。基本委员会认为，在关于电子零售产品和服务技术发展的监管事项和反应的持续反思与讨论中，本文作了初步的工作。

基本委员会将把本文件分发给全球内的监管者，以期推进对电子银行和电子货币交易的风险管理的适当监管方法的发展。监管者则可能希望将该文件在其所辖的机构中流传。

本文的讨论是一般性的，因为有关电子银行和电子货币的技术瞬息万变，未来的产品和服务可能会与今天所用的产品和服务有天壤之别。在当前电子银行和电子货币交易发展的这一相对早期阶段，许多方面的风险既不能完全辨别得出，也不是可轻易估量的，不成熟的监管办法会有扼杀这些领域内的革新和创造的危险。所以，监管人必须鼓励银行建立一种足够严密的综合风险管理机制，来处理已知的重大风险，且这种机制有足够的弹性以适应电子银行和电子货币交易中相关的重大风险类型和强度的变化。这种风险管理机制仅在其不断发展时才是行之有效的。

本文的其余部分安排如下。引言的下一部分阐述电子银行和电子货币的定义，以及银行作为电子货币交易中的参与者所扮演的重要角色，并指出了银行作为电子货币交易参与者所起的重要作用。第二部分则对电子银行和电子货币可能为银行业带来的风险进行分类。对风

^①资料来源：BCBS, 1998: Risk Management for Electronic Banking and Electronic Money Activities, Basle Committee on Banking Supervision, March 1998 BS/97/122.

险的分类和分析并不要求详尽无遗，本文旨在说明银行可能遇到的风险类型。其中，分析部分揭示：经营风险、信用风险和法律风险最可能发生。¹

随着电子银行和电子货币的不断发展，银行和用户间的跨国交易将会增加。这种关系可能给银行和监管人带来不同的问题和风险。为此，第二部分还讨论了有关跨国交易风险的问题。

基于对风险的区别和分析，第三部分为从事电子银行和电子货币交易的银行指出了风险管理过程的主要步骤，包括评估风险、执行风险披露措施和监控风险三个方面。

1.2 电子银行和电子货币的定义

1.2.1 电子银行指通过电子通道供应零售和小额金融产品和服务²。上述的产品和服务可以包括：存款、借贷、帐户管理、提供财务咨询、电子帐单支付和其他电子支付产品和服务的供应，例如电子货币（在下文单独界定）。

电子银行包括两个基本方面：进行交易活动的交割通道的性质以及顾客利用通道的方法。普通的交割通道包括“封闭”网络和“开放”网络。“封闭网络”通过关于成员条件的协议限制参与者进入（金融机构、客户、商家和第三方服务的提供者）。“开放网络”没有这样的成员身份要求。目前，广泛使用的用于提供给客户金融产品和服务的方法包括：销售终端点、自动柜员机、电话、个人电脑、智能卡和其他方法。

1.2.2 电子货币指用于通过销售终端、两种装置之间的直接转换，或者通过因特网之类的计算机网络进行支付的“储值”机制或预付机制³。储值产品包括“硬件”或“以卡为基础”的机制（又称“电子钱包”），和“软件”或“以网络为基础的”机制（又称“数字现金”）。储值卡可以是“单一卡”或“多功能卡”⁴。单一卡（例如电话卡）是用来购买一种货物或者服务，或来自一个卖主的产品，多功能卡是可以用于从数个卖主处进行各式各样的购买⁵。

银行可以作为发行人参与电子货币计划，也可以扮演其他角色。这些角色有：发行由其他实体发行的电子货币；为贸易商支付电子货币交易所得；办理电子货币交易手续、结算和清算；保存交易记录。

2. 风险的识别与风险分析

由于信息技术的迅速发展，难以详尽无遗地将风险一一列举。本文旨在阐述一系列广泛的有代表性风险，作为确定风险管理一般原则的基础。从事电子银行和电子货币交易的银行所面临的具体风险，可以根据巴塞尔委员会的其他风险管理文件中论述的风险类型归类，从这一意义上说，这些风险不是新发现的。用这种方式将风险归类有助于系统地确定银行组织所面临的风险。附件中列举了归入风险类型中的具体风险和问题，这些是银行在电子银行和电子货币业务中可能会遇到的。

尽管电子银行和电子货币引起的基本风险对人们来说不新鲜，但其中一些风险具体怎样产生，及其对银行的影响究竟有多大，对银行和监管者来说也许是个新课题。其中一些风险和问题可能是银行在电子银行和电子货币业务中都会遇到的，但是一种特定风险在不同电子银行和电子货币业务中的表现程度会有所差异。

目前，在大部分电子银行和电子货币业务中可能遇到的最重要风险是运作风险、信用风险和法律风险，对分散化的国际性银行尤其如此。下面三小节将讨论这些风险的具体表现形式。有些具体问题贯穿于各种风险之中。例如，允许未经授权而获得客户信息这一破坏安全检查程序的行为被归入运作风险一类，然而，这样的行为也使银行面临信用风险和法律风险。

尽管这些不同种类的风险可能是单由某个问题引发的,但有效的风险管理要求采取多种补救的方法,以应对每一种不同的风险。在其后的内容中,讨论了对某些电子银行和电子货币交易可能同样是重要的其他风险。本文还论述了跨越国界带来的潜在风险。

2.1 运作风险

运作风险来自系统严重缺乏可靠性或完整性而导致的潜在损失。由于银行的系统或产品可能受到内部或外部的攻击,安全性考虑是至关重要的。运作风险也可能因客户的滥用,及未经周密设计或未能有效运行的电子银行和电子货币交易系统而产生。此类风险的许多具体表现形式在电子银行和电子货币业务中都存在。

2.1.1 安全性风险

运作风险主要涉及进入银行的核心会计系统和风险管理系统的控制装置,与其他参与者交流的信息,及银行在电子货币业务中检测并制止伪造的措施。由于电子计算机功能的增强,线路入口点在地理上的分散性,以及包括因特网之类公共网络的各种通讯系统的使用,对进入银行系统的控制变得日益复杂化。必须指出,对于电子货币来说,破坏安全检查程序会导致采取不正当手段将责任强加于银行。至于其他形式的电子银行,未经授权的访问会导致直接损失,将责任强加于客户,或者引起其他问题。

各种具体的访问和认证问题也会发生,例如,控制不严会使黑客得以通过因特网组织一次成功的袭击,黑客可以获取、盗走、使用机密的客户信息。局外的第三方会在缺乏严格控制的情况下,进入某家银行电脑系统,并置入病毒。

除电子货币和电子银行系统所遭受的外部攻击外,银行还会由于员工欺诈而面临运作风险:员工可以在窃取认证数据后进入客户帐户,或偷取储值卡。员工因疏忽造成的过失,也会危及银行的系统。

监管机构直接关心的风险是伪造电子货币的犯罪。如果银行不能综合运用各种有效措施来检测并防范伪造,这种风险会更加突出。由于银行可能对伪造的电子货币结余金额承担责任,所以伪造会给银行带来运作风险。另外,修复受损的系统,也需要一定的费用。

2.1.2 系统的设计、运行与维护

银行面临其选择的系统设计不完善或运行不顺畅的风险。例如,若银行选择的电子银行或电子货币交易系统与客户的需求不匹配,银行的现存系统会有被中断或变得滞缓的危险。

许多银行很可能依靠外部的服务供应商和专家来运作、经营或支持其部分电子货币和电子银行交易。这种依赖也许是可取的,因为银行在其自身提供电子银行和电子货币服务并不太经济时,可以利用外部资源。然而,依靠外部资源会使银行面临运作风险。服务商有可能不具备必要的专业技术向银行提供其所需要的服务,或不能及时更新技术。服务供应商的经营会因系统中断或财政困难而间断,从而影响银行供应产品或服务的能力。

由于信息技术的发展日新月异,银行面临系统被淘汰的风险。例如,帮助客户使用电子银行和电子货币产品的软件需要更新,但是,罪犯或有预谋的个人可能利用更新软件时使用的通道拦截数据或修改软件。除此之外,迅速的技术革新意味着银行的员工可能无法充分认识新技术的实质。这会引发新系统或旧系统中的运行问题。

2.1.3 客户滥用产品和服务

与传统银行业务一样,客户的滥用,无论是有意还是无意,都会导致运作风险。如果银行不能对其客户进行适当的安全预防培训,风险可能更大。此外,如果缺乏有效的方法确认

交易，客户就可能否认其先前认可的交易，使银行遭受损失。在缺乏安全保证的电子交易中，客户使用个人信息（例如验证信息、信用卡号或银行帐号）有可能使犯罪分子乘机进入客户的帐户。最终，银行可能因为客户否认该交易而遭受损失。洗钱是另一个值得关注的风险来源，1997年4月的《十国集团报告》（电子货币：客户保护、法律实施、监管和跨国界风险）指出了这一问题。

2.2 信用风险

信用风险是指有重大影响的负面舆论风险，会导致资金筹措或客户群方面的重大损失。信用风险可能包括一些导致公众对整个银行的运营持续的消极印象的行为，致使银行建立和维护客户关系的能力严重受损。如果银行的行为使公众对银行履行其持续运营所必需的基本职能严重丧失信心，也会出现信用风险。信用风险可能是由银行自身的行为引起的，也可能是由第三方的行为引起的。在其他类型的风险中，尤其是运作风险中，风险日益频繁地出现或问题的增加，可直接导致信用风险加大。

当系统或产品不能如预期的那样运作，并导致公众广泛的消极反应时，就会产生信用风险。一次重大的安全事故，无论由于银行系统受到内部还是外部的攻击，都会影响公众对银行的信心。如果客户在接受服务过程中遇到问题，却得不到关于产品使用和问题解决方案的充分信息，也会引起信用风险。

过失、渎职及第三方欺诈都会使银行面临信用风险。如果通讯网络系统出现重大故障，妨害客户使用他们的资金或帐户信息，就会产生信用风险，尤其是没有其他访问帐户的替代方法可用时。其他提供相同或相似的电子银行和电子货币产品或服务的机构因过失引起重大损失，会使银行客户对其提供的产品和服务产生怀疑，即使银行自身并不存在类似问题。对某家银行有目的的攻击也可能带来信用风险。例如，侵入银行网站的黑客，可能对这个网站作些改动，故意散布关于银行和其产品的错误信息。

信用风险不仅仅对单个的银行可能是重要的，而且对于作为一个整体的银行系统都至为关键。举例来说，如果一家全球性的银行在电子银行和电子货币业务上遭遇严重的信用危机，会引起人们对其他银行的系统安全性的怀疑。在极端情况下，上述的情形会导致整个银行业系统的崩溃。

2.3 法律风险

法律风险产生于违反法律、法规、规章或交易习惯，或者与之不一致，或交易各方的权利和义务未能合理分配的情况。由于许多零售电子银行和电子货币交易相对较新的特性，在某些情况下，这些交易的各方权利义务是不确定的。例如，在一些国家，某些客户保护规则在电子银行和电子货币交易中的具体适用并不明确。此外，通过电子媒介订立的协议效力不确定，也可能引起法律风险。

如果电子货币系统的结算和交易限制较少，对交易不作严格的审查，会给洗钱者以可乘之机。对一些形式的电子支付，洗钱规则也许不适用。由于电子银行可以进行远程操作，银行用传统的方法来防范和查明犯罪行为会遇到更多的困难。

在向客户披露事实和保护隐私方面，从事电子银行和电子货币业务的银行也将面临法律风险。未被适当告知权利义务的顾客可能将银行告上法庭。在一些国家，未提供充分的隐私保护也会使银行受到监管许可的限制。

为了更好地向客户提供服务，有的银行将其网站与其他网站链接，这样也会带来法律风险。黑客可能利用被链接的网站欺诈银行的客户，而银行会被客户告上法庭。

随着电子商务的发展,银行会力求在电子认证系统中占有一席之地,例如使用数字证书。认证机构的角色也会使银行面临法律风险,例如,赔偿那些信赖证书的各方所遭受的损失。另外,如果银行参与一个新的认证系统,而双方的权利义务又未能在合同中明确,法律风险可能接踵而至。

2.4 其他风险

传统的一些银行风险,如信贷风险、流动风险、利率风险、市场风险也都会出现在电子银行和电子货币交易中,但对银行和监管者来说,这些风险与运作风险、信用风险、法律风险的实际后果的重要性是不同的。相比那些专门从事电子银行和电子货币交易的银行或银行的附属机构,从事多种银行业务的那些银行更是如此。

2.4.1 信贷风险是指相对方在债务期满或期满后不能清偿的风险。从事电子银行业务的银行会通过非传统的渠道提供贷款,并在传统的地理疆域外开拓市场。对于通过远程银行业务程序申请贷款的借款人,如果确定其信用额度的程序不当,会加大银行的信贷风险。从事电子票据支付业务的银行,可能因某个第三方中介机构不履行付款义务而遇到信用风险。假如电子货币的发行人怠于履行赎回义务,从该发行人处购得电子货币以转售给客户的银行,就会卷入信用风险。

2.4.2 流动风险是指银行无力偿还到期债务的风险,但并未造成不可挽回的损失,银行最终有可能履行其付款义务。对那些专门从事电子货币业务的银行,如果不能备有充足的资金随时供赎回和结算之用,此时,流动风险值得关注。再则,不能及时满足赎回的需求,会引发对机构提起的诉讼,使信用受损。

2.4.3 利率风险是指利率的不利变动对银行财务状况的影响。如果利率的不利变动致使与未清偿的电子货币债务相关的资产贬值,专事于电子货币供应业务的银行将面临严重的利率风险。

2.4.4 市场风险是指由于市场价格的波动,包括外币汇率的波动造成表内损失和表外损失的风险。在电子货币支付中接受外币的银行会面临此种风险。

2.5 跨国界风险

电子银行和电子货币交易基于一种旨在拓展银行和客户的地理范围的技术。此类市场的扩张跨越国界的同时,也伴以某些风险的凸显。尽管目前银行在国际业务中也遭遇类似风险,但有必要指出,这些风险与从事跨国界的电子银行和电子货币业务有关。当银行跨越国界与客户进行业务往来时,会遇到不同的法律、惯例上的要求。对于新型的零售电子银行服务,例如网上银行,以及对于电子货币,一些国家的法律要求缺乏稳定性。此外,不同的国家机构的管辖权可能模棱两可。这些因素会使银行因不能遵循不同国家的法律、法规而招致法律风险,这些法律和法规包括:消费者保护法,记录保存和报告要求,隐私规则和洗钱法。

银行与处于其他国家的服务供应商来往可能要面对运作风险,因为在这种情况下,监控更困难。跨国提供电子银行和电子货币业务服务,也会使银行面临其他风险。银行在电子银行和电子货币业务中与处在国外的服务供应商或外国参与者打交道时,可能遇到国家风险,因为外方会受经济、社会或政治等因素影响,无法履行其义务。通过因特网之类的开放网络提供服务的银行,由于难以用建立在更为熟悉的客户基础上的程序评估在其他国家的客户提出的贷款申请,可能会因此而面临信贷风险。兑付电子货币时接受外币的银行可能由于外币汇率的变动遭受市场风险。

3. 风险管理

越来越多的银行可能出于战略考虑从事电子银行和电子货币业务。而且，广泛使用电子银行和电子货币会提高银行和支付系统的效率，使客户和商家受益。但是，正如前文所述，从事电子银行和电子货币业务是有风险的。因此，必须使利益与风险平衡；银行必须有能力和控制风险，如有必要，还得承受相关损失。银行也要比照所面临的其他风险，权衡电子银行和电子货币业务中的风险。尽管电子银行和电子货币业务在银行当前的全部业务中仅占较小的一部分，但监管者可以要求高级管理层确保关键系统不受银行遭受的风险的威胁。

迅速的技术革新会改变银行在电子银行和电子货币业务中面对的风险性质与范围。监管者希望银行能拥有一套既能应对已有风险，亦能适应新风险的管理机制。包括风险评估、风险控制及风险监测这三要素的风险管理机制有助于达到上述目标。从事新的电子银行和电子货币业务，以及评估当前在这些业务中承担的义务时，银行可以采用这样一套机制。

银行有必要拥有一套综合的风险管理机制，置于董事会和高级管理层的适当监管之下。电子银行和电子货币业务中的新风险一经确认和评估，必须告知董事会和高级管理层。在开展新业务前，必须进行综合审查，以使高级管理层确保风险管理机制足以评估、控制和监测拟开展的新业务中出现的风险。

3.1 风险评估

风险评估是一个持续的过程。一般来说，它包括三个步骤。首先，银行可通过一个严格的分析过程来识别风险，并在可能的情况下使之量化。如果无法将风险量化，管理者仍可以确定潜在风险是如何产生的，以及应对和限制风险的措施。银行管理者应当作出可行的合理判断，确定风险对银行的影响程度（包括最大限度的潜在影响），以及此类事件发生的可能性。

评估风险的第二步是，董事会或高级管理层在评估某一具体问题发生时银行所能承受的损失基础上，确定银行的风险承受力。最后，管理者可以比较银行的风险承受力与评估出的风险严重性程度，以确定银行面临的风险是否在其承受范围内。

3.2 风险管理与风险控制

在对风险和风险承受力作出评估后，银行管理者应采取措施管理和控制风险。风险管理过程的这一阶段包括如下活动：贯彻安全政策和措施，协调内部的交流，评价并改良产品和服务，执行用来保证利用外部资源产生的风险得到管理和控制的措施，披露信息并提供客户培训，以及准备紧急应对方案。高级管理层应确保负责实施风险控制措施的员工独立于负责电子银行或电子货币业务的部门。通过将政策和程序以书面文件的形式确定下来，并使有关的员工都能够利用这些文件，银行会提高其控制和管理各种业务活动固有风险的能力。

3.2.1 安全政策和措施

安全是用以保证数据和操作过程的完整性、可靠性和机密性的系统、应用程序和内部控制措施的有机组合。真正的安全依赖于就银行内部的程序和银行与外部的交流确定有效的安全政策和安全措施，并付诸实施。安全政策和措施可以防范电子银行和电子货币系统受到内部和外部攻击的风险，控制由于破坏安全检查程序引起的信用风险。

一项安全政策要阐明管理者保证信息安全的意图，并说明银行的安全体制。安全政策也确立用来确定银行风险承受力的指导方针。它可以明确设计、贯彻和执行信息安全措施的职责，并确定一些程序来评估政策的遵守情况，贯彻规章制度，并报告破坏安全的行为。

安全措施是硬件、软件工具和人事管理的结合，有助于建立可靠的系统并保障正常的营运。高级管理层应当意识到，安全是一个系统工程，维系于其中最的薄弱环节。银行可以在

各种安全措施中作出选择，预防或缓解来自内部和外部的攻击，减少对电子银行和电子货币的滥用。此类手段包括加密、加设口令、防火墙、病毒过滤和员工筛选等。加密是使用密码规则将明码文本数据转换成密码数据以防未经授权的浏览。访问控制和用户识别的技术有口令、通行用语、个人识别号、附在硬件上的标志和生物统计学等。

防火墙是软件和硬件的结合，它们审查并限制经外部通路访问与开放式网络(如因特网)相连的内部系统。防火墙也可以利用因特网技术分割内部网(局域网)。如果防火墙技术得到正确的设计与运用，它将成为控制访问并保证数据机密性和真实性的有效手段。因为这种技术的设计复杂，成本较高，它的强度与性能应当同将被保护的信息的敏感度相称。一项设计周全的方案应涵盖整个企业的安全要求、清晰的运作程序、责任分工，以及将被委任负责防火墙的配置和操作的员工的挑选。

尽管防火墙过滤进入的信息，但是，它们并不一定对从因特网下载的被病毒感染的程序存有戒备。因此，管理者应该建立预防和检测机制以减少感染病毒和数据被破坏的可能性，尤其是对于远程银行。减少感染病毒的风险的方法有网络控制、终端用户政策、用户培训和杀毒软件。

并非所有的安全威胁都是外在的。还应当尽可能防备现任或已离任雇员未经授权的行为，以保护电子银行和电子货币系统。就现有的银行业务来说，对新雇员、临时雇员和顾问进行背景调查，以及内控和责任分工，都是保证系统安全的重要防范措施。

这样的措施包括与发行人或中心操作员的在线互动；监控和追踪个别交易；将累积的交易记录保存于中央数据库；在储值卡和商用硬件中使用防篡改装置；在储值卡中设定价值限额和有效期限。

3.2.2 内部沟通

如果高级管理层让核心员工认识到电子银行与电子货币服务如何支持银行的整体目标，那么运作风险、信用风险、法律风险和其他方面的风险是可以管理和控制的。同时，技术人员应向高级管理层说明系统是如何设计、运行的，以及系统的优点与缺陷。这些程序可以减少由于系统设计不完善导致的运作风险，包括银行组织内部不同系统之间的冲突；数据完整性问题；由于系统不正常运行引起客户不满导致的信用风险，以及信贷风险和流动风险。

为确保充分的内部交流，所有的政策和程序必须以书面形式规定下来。此外，高级管理层应当制订有关继续教育和技能与知识更新的内部政策，跟上技术革新的步伐，减少由于专业技术人员匮乏和管理经验不足导致的运作风险。培训可以包括技术课程，给予员工把握重要市场发展情况学习时间。

3.2.3 评估与升级

在全面推广之前对产品和服务进行评估，也有利于控制运作风险和信用风险。通过测试可确认设备和系统正常运作，并产生预期的结果。模拟程序或模型有助于开发新的应用程序。定期测试现有硬件和软件的性能可以减少系统滞缓或者中断的风险。

3.2.4 利用外部资源

在银行业中有这样一种愈演愈烈的趋势，银行的战略重点纷纷集中于核心竞争力，并且依赖于具备银行专门技能之外专长的外部参与者。尽管这些安排有助于降低成本，实现规模经济效益，但利用外部资源并未解除银行的最终责任，它们依然要负责控制那些影响其运作的风险。因此，银行应该采取措施，以减少由于依赖外部服务供应商所引起的风险。例如，银行管理者应监控其服务供应商的经营活动和财务状况；确保双方之间的合同关系与各自的

预期目标和义务，得到准确无误的理解，并以可强制执行的书面形式确定下来，而且，如有必要，随时准备在紧急情况下迅速更换服务供应商。

银行机密信息的安全至关重要。外部资源的利用可能要求银行与服务供应商共享机密信息。银行管理者应该审查服务供应商保护机密信息的政策和程序，从而评估服务供应商是否能够提供如同在内部进行业务活动一样的安全保障。此外，在必要的时候，监管者可以有权独立地评定服务供应商的能力、经营活动和财务状况。

3.2.5 信息披露与客户培训

信息披露和客户培训有助于减少银行的法律风险和信用风险。关于如何使用新产品和服务、产品的价格和服务费用、问题和差错的解决方案等的信息披露和客户培训制度，可帮助银行遵守保护消费者和隐私的法律和规定。披露并解释银行与链接网站的关系有利于减少银行由于相链接网站的产品和服务出现问题而面临的法律风险。

3.2.6 应急方案

通过建立紧急应对计划，确定在电子银行和电子货币服务供应中断的情况下的行动方案，银行可以减少内部程序或者服务或产品供应中断的风险。该计划可以包括数据恢复，交互数据处理能力，应急人员，以及客户服务支持。对备份系统应进行定期检测，确保连续地有效运作。银行应保证紧急情况下的运作与正常经营时一样安全。

电子银行和电子货币的一个重要方面是对包括硬件销售商、软件供应商、因特网服务供应商和电信公司在内的外部实体的依赖。银行的管理者可以要求上述服务供应商具有备份的能力。另外，管理者可以考虑在服务供应商遭受损害时进行索赔。此类方案可以包括与其他供应商之间的短期契约，以及规定如何处理由于服务中断造成的客户损失的政策。银行也应该考虑权利保留这一明智做法，在必要时立即更换服务供应商。应急方案也有利于控制由于银行自身行为，或者由于提供相同或类似电子银行或电子货币产品或服务其他机构遇到的麻烦导致的信用风险。例如，银行可以考虑建立系统中断时的客户问题处理程序。

3.3 风险监控

对任何风险管理来说，持续的监控都是非常重要的。就电子银行和电子货币业务而言，监控尤其重要，这不仅因为业务的性质可能随创新而迅速变化，也因为一些产品有赖于使用因特网之类的开放式网络。系统监测和审查是监控的两大要素。

3.3.1 系统监测与监督

监测系统的运作可以检测到不正常的活动模式，并帮助消除主要的系统问题，防止中断和受到攻击。尝试着有控制地进入正常程序之外的系统这种侵入监测，重点在识别、隔离和查证设计与安全机制实施中的缺陷。监督是监控的一种形式，它用软件和审计手段来追踪活动。与侵入监测不同，监督的重点是监控常规运作，调查异常活动，通过检测安全政策的执行情况对系统的安全性作出连续的判断。

3.3.2 审查

审查（包括内部和外部）是检测电子银行和电子货币业务中的缺陷并使风险最小化的重要独立控制机制。审查者的作用是保证银行确立并始终遵守适当的标准、政策和程序。为进行准确的检查，审查人员应当具备充分的专业技能。内部的审查员应该是独立的，与作出风险管理决策的人员分开。为加强内部审查，管理者可以聘请合格的外部审查人员，例如电脑安全顾问或其他有相关经验的专业人士，对电子银行或电子货币业务进行独立的评估。

3.4 跨国风险管理

跨国界风险要比银行在本国内面临的风险更复杂。因此，银行和监管者须投入更多的精力去评估、控制和监管在跨国电子银行和电子货币交易活动中发生的运作风险、信用风险、法律风险和其他风险。

有意向不同国家市场中的客户提供服务的银行，需要理解不同国家的法律要求，并对不同国家的客户对产品和服务的期望和认识差异，有一个正确的判断。此外，高级管理层应当保证，现有的信用延期和流动管理系统能够应对跨国业务活动带来的潜在困难。银行可能需要评估国家风险并制订应对突发事件的计划，处理由于国外经济问题或政治事件而导致的服务中断问题。银行也许会遇到强制国外的服务供应商履行义务的困难。如果银行依赖于国外的服务供应商，国家监管者可以要求逐一地评估跨国服务供应商的业务活动及其信息的可靠性。

在讨论管辖权争议和确定管辖权时，国家监管者可以发挥重要的作用。他们也可以继续努力，采取措施检测不安全和非法的行为。最后，国家监管者可以在共享有关产品和服务的革新与行业惯例的信息方面，再接再厉，加强合作。