2015 年 5 月

内部控制与风险管理信息简报

目 录

DIB 数据库中心

2015/06/08

内控动态

银监会发布《关于加强银行业金融机构内控管理有效防范柜面业务操作风险的通知》

来源：银监会　　整理：研究部

近期，全国发生多起存款纠纷事件，其中暴露出部分银行业金融机构存在内控制度执行不力、员工管理不到位等问题。银监会正依法对责任银行进行立案查处，严格按照相关规定处罚当事人和责任人，为全行业重敲警钟，确保客户合法权益和银行业合规经营。同时要求各银行业金融机构进行全面风险排查，梳理业务流程，深查严纠管理漏洞。为推动银行业金融机构规范运营，特别是有效防范柜面业务操作风险，银监会于 2015 年 6 月 5 日发布《关于加强银行业金融机构内控管理 有效防范柜面业务操作风险的通知》（以下简称《通知》）。

《通知》共 20 条，分别从制度顶层设计、重点环节防控、客户服务管理、危机处置以及加强监管等方面提出了具体要求。

第一，严守业务管理、风险合规及审计监督“三道防线”，加强内控体系建设，落实主体责任。针对开户、资金汇划、对账、印章凭证管理及账户监控等五个柜面业务关键环节，提出明确具体的监管要求。同时《通知》要求，对前期出现较多消费纠纷的代销业务，银行业金融机构要通过集中上收代销业务审批权限，对代销机构实行名单制管理以及加强代销产品信息的公开公示等措施加强管理，特别强调要加强对客户个人信息安全的保护。

第二，重点领域严密设防，更加强调过程管理和行为管理。一是要“看好自己的门”、“管好自己的人”，加强营业场所和员工行为的管理。银行业金融机构近期要组织开展一次重点岗位员工行为专项大排查，对发现的问题及时采取相应措施，严肃整改。二是加强技术防控，在营业网点现金区全面实施同步的录音录像，加快推进银行理财产品和代销产品销售的录音录像工作，记录业务办理的全过程，加强监控员工操作行为。

第三，加大问责力度，确保已经发生的风险事件处置的程序公平、方式合理、结果公正。实行涉事机构所在一级分行和总行业务条线的双线查处及双线整改问

责。在对风险事件直接责任人进行严肃问责的同时，对管理不尽职、履职不到位的机构负责人和业务条线管理人员也要严格认定责任并严肃问责。对于性质严重、负面影响大的风险事件，要比照案件问责标准严肃问责，绝不姑息，并建立内部举报核查制度。

第四，加强对社会公众的服务和宣传。提示公众强化“五个警惕”，即警惕高息诱惑，警惕资金捐客，警惕他人代办，警惕附加承诺，警惕信息泄露，进一步提高公众资金和信息安全的自我保护意识。

政策解读

联交所刊发有关审阅发行人年报披露内容监察其合规情况的结果

来源：香港交易所　　整理：研究部

2015 年 3 月 27 日，香港联交所就其审阅上市发行人年报（财政年结日截于 2013 年 12 月至 2014 年 11 月之间）所得结果和建议刊发报告。

审阅发行人年报披露内容为联交所的定期监察活动之一，旨在检视发行人在遵守《上市规则》方面的合规情况、发行人的企业操守及其对重大事件和发展的披露情况。联交所公布有关审阅结果并提出若干建议，以保障市场的公平有序和讯息透明。

联交所是次审阅发行人年报所涵盖范围包括：透过发行股本证券/可换股证券及认购权进行集资、收购后发生重大变动的更新资料、收购项目业绩表现保证的结果、发行人财务表现的重大变动、采纳香港财务报告准则第 10 号/国际财务报告准则第 10 号、生物资产、于 2012 年及 2013 年上市的发行人、根据《主板规则》第十八章/《创业板规则》第十八 A 章有关矿业或石油资产的定期披露。此项审阅与联交所的财务报表审阅计划不同。联交所的财务报表审阅计划就发行人有否遵守财务汇报准则及《上市规则》有关财务资料的披露，审阅发行人的定期财务报告。

联交所从年报中注意到发行人在上述方面的披露均见进步，亦注意到涉嫌严重违反《上市规则》的个案有所下降。联交所特别指出，希望发行人在以下方面能够继续改善讯息披露质量：

一、股本集资。从良好企业管治的角度考虑，进行股本集资的发行人应在集资时清楚披露预定的集资用途，并在年报中向股东汇报集资所得款项的实际用途。

二、发行人财务表现的重大变动。依赖主要客户的发行人，应在以下方面提供较深入的讨论：主要客户的详情及与其的关系，以及（若适用）出现任何重大逾期应收款项的原因、发行人如何执行其信贷政策，以至有关减值拨备及年结日后结清情况的详情等。

应收货款出现重大变动的发行人，应在以下方面提供较深入的讨论：任何偏离发行人本身既定信贷政策的情况（譬如：债务人周转日数较一般信贷期长、若干客户获给更长的信贷期及该等客户的概况和彼此关系）、在年结日后结清的应收货款、以及发行人对逾期应收款项所采取的跟进行动。

三、新上市发行人。根据内幕消息条文刊发盈警公告的新上市发行人，应确保有关内容属招股章程日期后所出现的重大发展而发行人尚未披露的资料。发行人若拟向市场提供关于其上市后财政状况且不属内幕消息的额外资料，应确保该等资料有意义且具体，而非重述招股章程中的披露（譬如披露具体财务数据）。此外，发行人亦应选择适当的标题类别来描述此等资料性质。

香港交易所集团监管事务总监兼上市科主管戴林瀚说："我们乐见发行人参考了我们往年的指引且加强了讯息披露和对股东的责任意识。透过这项审阅和我们的查询及跟进，发行人在年报披露质素及《上市规则》合规方面均见改善。"

因此，发行人在编制年报时应注意联交所在报告内提出的审阅结果和建议，并采纳其中的指引。

行业案例及风险提示

互联网企业频现“宕机门” 敲响网络安全警钟

文：DIB 研究部

五月似乎是互联网公司的“黑色五月”，陆续有网易、支付宝、携程等大型互联网网站“宕机”。

首先，5 月 11 日晚上 9 时，网易突然出现大面积服务瘫痪问题，网易旗下的新闻、易信、云音乐、有道云笔记等多款互联网+产品以及全线游戏皆出现了网络中断的情况，长时间无法刷新和登录。有传言称网易总部着火爆炸。当晚 9 点 42 分，网易官方回应，称是骨干网络遭受攻击所致，正在抢修，恢复时间待定。同时澄清，关于网易大厦着火的新闻为谣言。直到第二天凌晨 2 时 30 分，网易方面才表示，经过工程师团队的紧急抢修，故障已被排除。

尽管网易网络和相关服务已恢复正常，但有媒体粗略统计，超过 1 亿名以上用户受到网易此次宕机事故影响，而在其中游戏用户人数至少超过 400 万人。此次宕机对网易的收入将带来巨大影响，根据网易 2014 年四季度财报数据，网易游戏服务的收入高达 28.63 亿元，平均每天收入 3000 万元。按照这样来估算的话，网易本次的大面积宕机，单是游戏就会带来直接经济损失超过 1500 万元。

就在网易网络瘫痪前一天，社交软件陌陌也在微博上宣布，“5 月 10 日当晚，由于网络故障，陌陌暂时无法正常使用”。经查，也是因骨干网络受到攻击所致。

之后，支付宝出现网络故障。5 月 27 日下午 17 时左右，全国多地网友反映支付宝出现故障，无法登陆，手机和电脑版支付宝均无法正常使用，支付宝钱包登陆页面显示“请求超时，请稍后再试”字样。对此，支付宝官方回复称，此次故障是由于杭州市萧山区某地光纤被挖断所致。到晚上 19 时多，支付宝宣布用户服务已经恢复正常。

紧接着，携程也“中招”了。5 月 28 日上午 11 时许，携程网站突然陷入瘫痪，打开主页后点击时均显示“Service Unavailable”，百度搜索上携程官方页面也显示 404 错误，App 亦无法使用。12 时，携程发表声明：今天上午 11:09，部分服务器遭到不明攻击，正在紧急恢复。到 15 时，携程网主页可以访问静态

页面，但提示“携程网暂时无法提供服务，正在紧急修复中，您可以访问艺龙旅行网”。大量流量被导到携程刚刚收购的艺龙。

然而，当天 17 时许，艺龙阶段性地“挂了”，出现短暂无法访问的情况。艺龙 CEO 崔广福表示，艺龙网首页受到流量攻击，并已报案。随后，携程流量停止导向艺龙，之后不久艺龙又恢复导流。20 点左右，网站、App 程序恢复，但大部分产品仍然无法预订。22 点 45 分，携程表示：经技术人员抢修，除个别业务外，携程官方网站及 App 恢复正常。经过排查，携程郑重声明数据没有丢失，预订数据也保存完整。直至当天 23 时 29 分，才全面恢复正常。经携程技术排查，确认此次事件是由于员工错误操作，删除了生产服务器上的执行代码导致。

携程此次宕机，从发现到全面修复超过了 12 个小时。据携程一季度财报估算，携程的直接损失是每小时 106 万美元左右，以 12 小时计算总损失超过 1200 万美元。

【行业风险提示】

作为 21 世纪信息化建设不断深入的产物，互联网是借助于光纤、电缆等高新技术手段互联而成的超大型计算机网络平台，互联网企业的主要业务与日常经营活动也都是通过这一平台得以实现。然而，构筑于网络安全协议之上的公共平台，其本身最大的特点便是开放性，这就使得相关的系统性信息安全隐患成为客观存在的必然，网络基础设施故障、软件漏洞、链路中断、甚至包括恶意攻击引起的整个网络瘫痪的问题，已经越来越成为困扰互联网企业发展的关键环节。

具体来说，部分以阿里为首的互联网公司惯于采用 UNIX 系统主机终端模式，而 UNIX 系统未提供主机与终端之间的通讯加密，它本身是一个开放的系统，并且其源代码已经公开，因而存在极大的安全隐患，本次“宕机”事件主角之一的网易便已深受其害，一旦恶意攻击者通过破译进入了系统内核程序，整个网络平台无可避免的将遭受“毁灭性”打击；其次，是网络 TCP / IP 协议安全性差，缺乏对网络行为的有效约束，网络安全协议是基于道德层面的行为公约，缺乏法律约束的强制性，5 月 28 日的携程与艺龙瘫痪事件，不良分子公然破坏协议，对网站进行恶意攻击和肆意破坏，再一次将网络行为约束和信息安全纳入到了公

众视线焦点之内；除此之外，防火墙安全性不高，部分互联网企业缺乏有效的技术支撑，网络攻击防范也只是简单的采用上网行为管理 AC（Access control）及其内置的防火墙来实现，措施相对薄弱，也是导致网络信息安全问题发生的重要因素之一，作为互联网企业的龙头代表，阿里、网易、携程等网站如此轻易的被攻击成功，甚至造成长达 12 小时的系统瘫痪，其系统服务器的防御能力不得不让外界产生疑问；最后，缺乏相应的网络数据灾备与恢复机制 ，不少企业只是简单的通过磁盘整列采用 RAID5 技术来实现数据备份与恢复，而随着设备的长期使用，一旦发生多个磁盘同时损坏的现象，就会造成大量数据的丢失或外泄，不管是由于内部员工的失误操作，或者外部竞争者的恶意攻击，信息的保密性均是客户最为关注的问题，尽管已经对宣称对系统服务器进行了二次优化，但如携程般多次的信息泄露和数据丢失事故已不得不让人对其数据灾备体系产生怀疑；

目前，虽然不少互联网企业都已采取了相关的安全措施，但信息化系统风险一旦发生，则很可能导致整个系统的瘫痪，从而给企业的声誉以及正常经营带来十分不利的影响。

在信息化开放程度越来越高的今天，互联网企业应当更加注重信息化系统风险的防范，对内，应努力优化物理硬件，提升技术团队，做好灾备应急与内部控制工作；对外，则需时刻警惕恶意攻击包括恶意竞争带来的不良影响，做好危机公关与企业形象的维护工作。

作为监管部门，应当在完善相关法律法规的同时，密切注意互联网行业网站的流量监测，一旦发现流量异常情况，应及时予以重点监控，对于重大互联网安全事件及时备案，对于恶意攻击行为，应予以相应的处罚。

DIB 内部控制与风险管理数据库

专注 专业 卓越

DIB 内部控制与风险管理数据库旨在为国内外各类型企业、研究机构、政府机构等提供内部控制与风险管理相关的数据与信息。该数据库目前包含风险库、内部控制库、案例库、法律法规库、内控动态、外部审计库、公司基本信息库 8 个大型专业数据库，27 个子数据库，内容涉及 200 多个细分行业，涵盖面较广，动态更新及时、准确。

了解更多

如需了解更多，可登入 DIB 内部控制与风险管理数据库宣传介绍网站，链接如下：请点击> http://www.ic-erm.com

销售冠监：熊女士 18676708100

销售座机： 027-87497827 转 8006/8008/

敬请关注迪博微信：迪博风控

公众号：dibcn-com