

德勤企业风险 第六辑

个人信息保护—— 应对法律合规要求，妥善处理个人信息

德勤企业风险管理服务部 编



Deloitte.
德勤



上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

德勤企业风险(第六辑)

个人信息保护 ——应对法律合规要求,妥善处理个人信息

德勤企业风险管理服务部 编



上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

内 容 提 要

本书是德勤企业风险丛书的第六辑，主要涉及个人信息保护的最前沿话题。内容包括如何通过数据丢失防护系统应对日益严格的信息保护法规及监管要求；个人信息保护立法及监管要求；个人资料保护制度建置；隐私保护的企业现状和合规挑战；管理数据隐私的利器——身份和访问管理；个人资料泄漏调查经验；企业敏感数据保护之道；银行信息科技安全风险管理探讨，等等。本书可为企业的个人信息保护提供理论基础和最佳实践。

本书适合企业管理人员、相关政策制定者以及研究者参考阅读。

图书在版编目（CIP）数据

个人信息保护：应对法律合规要求，妥善处理个人信息 / 德勤企业风险管理服务部编．

—上海：上海交通大学出版社，2013

（德勤企业风险．第6辑）

ISBN 978-7-313-09784-2

I．①个… II．①德… III．①隐私权—法律保护—研究 IV．①D913.04

中国版本图书馆CIP数据核字（2013）第111772号

个人信息保护

——应对法律合规要求，妥善处理个人信息

德勤企业风险管理服务部 编

上海交通大学出版社出版发行

（上海市番禺路951号 邮政编码 200030）

电话：64071208 出版人：韩建民

上海华业装潢印刷有限公司印刷 全国新华书店经销

开本：890mm×1240mm 1/16 印张：4.75 字数：130千字

2013年6月第1版 2013年6月第1次印刷

ISBN 978-7-313-09784-2/D 定价：30.00元

版权所有 侵权必究

告读者：如发现本书有印装质量问题请与印刷厂质量科联系

联系电话：021-63812710



前言

"O, wonder! How many goodly creatures are there here! How beauteous mankind is! O brave new world, That has such people in't!"

——William Shakespeare, The Tempest, Act V, Scene I

“神奇啊！这里有多少好看的人！人类有多么美丽！啊！美丽的新世界，有这样的人在里头！”

——威廉·莎士比亚《暴风雨》第五场，第一幕

随着经济的迅猛发展，科技的力量越来越大，沟通的方式越来越多，资讯的传播越来越自由，人与人的距离越来越近。生活在这个愈渐狭小的地球村，人与人之间的信息交流与传播似乎轻而易举，让我们能生活在这美丽的新世界（O brave new world, That has such people in't!）。然而在这看似自由发达的外表下，信息安全及隐私泄漏的问题却无孔不入地渗入人们的生活。

繁多的资讯传播途径给人们的生活带来众多便利，个人的隐私却在这样的环境下无所遁形。移动电话号码、网上银行密码、公司内部决策等，这些私密信息随时都有可能被利用、误用，甚至被盗用和滥用，导致人们隐私的暴露，公司机密的泄漏。这种将隐私公之于众的行为不仅给个人带来身心的伤害，更会导致公司名誉受损，业绩受创。

为了遏制隐私泄漏这一电子信息高速发展下的衍生物，国家政府机构及相关团体已出台相关法律法规，以保证个人隐私不被侵犯。德勤作为行业的先驱，凭借自身专业的知识和多年的经验，有责任创造一个安全的信息环境，一个隐私受保护的時代。当人们可以在这电子化的时代里真正享受科技发展和信息分享的好处时，他们定能由衷地赞叹：

“神奇啊！这里有多少好看的人！人类有多么美丽！啊！美丽的新世界，有这样的人在里头！”

顾问圣

大中华企业讯息管理主管
企业风险管理服务合伙人

德勤企业风险

德勤企业风险管理服务部 编

编委

刘伟杰
蒋黎虹
薛梓源
黄皓礼
陈嘉祥
林允纲
方 烨
谈 亮

执行编委

原国太郎
孙永杰
冯文珊
彭为德
赵 理
何 萍
庄宇杰
吴坚隼

编委助理

李 华

目录



特集

- 1 如何通过数据丢失防护系统（DLP）应对日益严格的信息保护法规及监管要求？
- 4 个人信息保护立法及监管要求
- 8 个人资料保护制度建置项目经验谈
- 10 个人信息保护趋势浅谈
- 13 企业因应个人资料保护的建议——基于组织、流程、信息科技层面
- 18 隐私保护的企业现状和合规挑战
- 20 管理数据隐私的利器——身份和访问管理
- 24 个人资料泄漏调查经验分享
- 26 企业敏感信息保护之道
- 34 银行信息科技安全风险管理探讨

特别寄稿

- 38 当前宏观背景下租赁行业的机遇、风险和创新

德勤专家多元视角

2013年中国保险业十大趋势与展望（上）

研究室

- 57 如何构建商业银行的数据分析能力
- 62 低碳审计——浅谈内部控制评价与经济责任审计工作的整合

连载

- 65 保险业风险管理小故事(5)——谁审批了那笔交易？
- 66 企业内部控制实务(9)——资金管理

如何通过数据丢失防护系统 (DLP) 应对日益严格的信息保护法规及监管要求？

谭锐坚 总监

德勤香港事务所
企业风险管理服务

近年，传媒经常报道有关机构泄漏机密信息和滥用个人信息的情况。例如，在零售商店的会员制度中，客户提供的个人信息被过度收集；另外，有金融机构在没有获得客户同意的情况下，与第三方共享客户个人信息作直接促销用途；以及有医疗机构曾经遗失了载有病人病历记录的U盘，继而导致资料外泄。很显然，被指控的机构因此对自己的声誉造成负面影响，最终可能会因为机构和客户之间缺乏信任而影响了他们的经营业绩。

以上个案使得大众的注意力转向机构如何保管机密信息和保存他们的个人信息。他们会质疑机构是否有任何有效和足够的控制，以保护这些信息的安全，从而避免未经授权的访问和使用不当的情况发生。

另一方面，机构可能也注意到大众对机构如何保护他们提供给机构的个人信息的关注。为了提供足够的信息保护，机构可能会考虑这样的问题：机构可否确保在有需要的时候提供适当的数据？机构可否控制数据的访问权限？机构可否保护数据，防止机构内部/外部的信息被盗窃？机构可否遵从相应的法律要求（如《隐私法》）来保护客户数据？机构是否正确保护信息管理的基础设施？机构可否采用新兴技术（如云计算和移动计算）？

一、信息保护的法规/监管要求

在信息保护的重要性在全球上升的同时，来自不同国家的政府及监管机构已推出了各自的信息保护条例，并已在自己的国家中实施。在亚太区中，一些国家和地区如新加坡、菲律宾、韩国、印度尼西亚、泰国和日本等近年都制定了自己的信息保护原则，并已在几个主要范围上作出限制和指引。包括获取信息的应用、信息采集及处理、信息的传输以及违例通知，等等。

（一）香港的《个人资料（私隐）条例》（PDPO）

早在1996年12月香港就已经通过并实施了一套名为《个人资料（私隐）条例》的法例，用以确保每个人的个人信息得到保护。《个人资料（私隐）条例》是香港首套信息保护和管理的法定条例。它主要可以概括为以下6个信息保障的原则：

- (1) 个人资料的收集必须与资料使用者的职能和活动有关，而收集的资料适量便可及以合法及公平的手法收集，并须告知收集的目的及资料的用途；
- (2) 须采取切实可行的步骤确保个人资料的准确性，并在完成资料的使用目的后，删除资料；

- (3) 限制个人资料使用于当初的收集目的或直接有关的用途上，否则必须先获得资料当事人的同意；
- (4) 须采取切实可行的步骤确保个人资料的安全，免受未获授权或意外的查阅、处理、删除、丧失或使用的影晌；
- (5) 制订及提供个人资料的政策及实务；
- (6) 个人有权查阅及更改个人资料。资料使用者应在指定的时间内依从查阅或更改资料的要求，除非条例订明的拒绝理由适用。

（二）《个人资料（私隐）（修订）条例》（PDPAO）

电子商务以及相关技术的快速发展，引致全球对信息保护及隐私的关注。为了配合形势，香港进行了《个人资料（私隐）条例》的检讨，分析当时现行的法规对保护个人信息的充分性，并于2012年6月在立法会上通过了《个人资料（私隐）（修订）条例》。

《个人资料（私隐）（修订）条例》修改了个人资料（私隐）条例的原有条文；尤其是把信息用作直接营销的机构，严格规定了该类机构对个人信息的使用的限制，特别是这样的信息的提供和销售。

1. 机构在直销方面的责任

在机构使用个人资料做直销前，须告知信息当事人，在取得其同意后方可使用其个人资料。而机构亦须明确告知信息当事人以下信息：拟使用个人资料的种类、该资料被用于何种类别的促销标的、提供途径，让当事人传达同意或不同意。如果机构希望把相关信息转移给第三方，则除了上述的项目以外，还须以书面形式提供该信息，并告知在信息转移中是否牵涉任何金钱利益的有关事项。

2. 外包个人信息处理

当机构请求信息处理方对信息进行处理时，不管处理方是在香港或香港以外的地方，原机构应该与信息处理方签订一份合同以防止传输的信息保存超过所需的时间。合同条款也应防止由意外导致的未经授权的访问或更改（如删除），或信息丢失和未经授权的修改。

3. 违反《个人资料（私隐）（修订）条例》的刑罚

至于刑罚方面，如果违反了《个人资料（私隐）（修订）条例》，由于得到信息当事人的同意在条例中是最为重要的一个实际步骤，因此处罚主要根据这一项目而设立。如机构在



没有得到信息当事人同意的情况下披露个人信息，根据该条例，这是一个新的刑事罪行。触犯者可以被处以最高罚款达港币50万元及监禁长达3年。此外，如果信息在没有获得信息当事人授予的有效同意下被“售卖”给第三方，触犯者会被罚款港币100万元及最高刑罚为监禁5年。

(三) 中华人民共和国国家标准（国标）

中国国家标准化管理委员会亦于2013年2月1日实施了中华人民共和国国家标准，该法规旨在治理和保护个人信息的使用。其中的原则覆盖了将所有或部分个人信息输入到信息系统的过程。它适用于所有组织和机构以外的有公共管理职责的政府部门或类似机构。国标还指出，个人信息可以分为个人一般信息和个人敏感信息，并引入默许和明确同意的概念。国标也列明了机构收集和使用信息的8项基本要求，包括：

- (1) 须清楚告知信息当事人使用信息的目的；
- (2) 收集的信息不可超过必要的范围；
- (3) 明确披露收集信息的目的；
- (4) 须征得信息当事人的个人同意；
- (5) 确保信息质量保证；
- (6) 确保信息获得保护；
- (7) 执行诚信；
- (8) 须清楚界定明确责任。

在国标中，对用户的信息、信息当事人及第三方监测机构的角色进行了明确规定。包括信息当事人的权利、机构的责任、信息持有者删除信息的责任和第三方监测机构的基本成效。它也清楚地定义了信息处理周期的顺序，并将其依次分为4个阶段：信息收集、信息处理、信息传输和信息删除。

此外，国标有八大原则，用以标出重点领域范畴，当中包括：

- (1) 目的明确原则。处理个人资料要有特定、明确、合理的目的，不扩大使用范围，不在个人资料主体不知情的情况下改变处理个人资料的目的；
- (2) 最少够用原则。只处理与处理目的有关的最少资料，达到处理目的后，在最短时间内删除个人资料；
- (3) 公开告知原则。对个人资料主体要尽到告知、说明和警示的义务。以明确、易懂和适宜的方式如实向个人资料主体告知个人资料的处理目的、个人资料的收集和使用范围、个人资料的保护措施等；

- (4) 个人同意原则。处理个人资料前要征得个人资料主体的同意；
- (5) 品质保证原则。保证处理过程中的个人资料保密、完整、可用，并处于最新状态；
- (6) 安全保障原则。采取适当的、与个人资料遭受损害的可能性和严重性相适应的管理措施和技术手段，保护个人资料安全，防止未经个人资料管理者授权的检索、披露及丢失、泄露、损毁和篡改个人资料；
- (7) 诚信履行原则。按照收集时的承诺，或基于法定事由处理个人资料，在达到既定目的后不再继续处理个人资料；
- (8) 责任明确原则。明确个人资料处理过程中的责任，采取相应的措施落实相关责任，并对个人资料处理过程进行记录以便于追溯。

二、机构面对信息保护方面的挑战

如今，许多机构已经实施了监控系统来识别机密信息和传输过程中的信息交换，以防止信息丢失。然而，这些措施仍然可能存在一些漏洞，如监控系统可能无法正确识别机构的机密信息，或者它是否能适当地为机密信息进行加密，这仍然是一个值得机构认真考虑的重点。

机构的个别员工也可能被其他人提供的一些好处所引诱，而有意或无意地泄露了相关的个人信息，而那些则将该信息用在非法的用途上。例如，将一个包含间谍软件的电邮或U盘存入电脑以获得一个抽奖机会或赢得购物优惠券，等等。人们很容易因为未察觉而掉进这样的陷阱，从而被欺骗并无意地泄漏了信息。

三、数据丢失防护系统(DLP)

在过去的几年中，机构的日常业务运作对电脑系统的依赖日益增长，大量的信息传输是十年前所无法比拟的。加上信息系统的复杂性不断增加，数据丢失或泄漏信息的风险比过去更容易发生。

对于任何机构，数据泄漏/亏损都是不可接受的，因为它往往会导致机构受到财务及声誉/公信力的损害。在丢失/泄漏敏感数据的情况下，机构甚至面对诉讼的可能性。

为了防止发生上述损失，机构可以部署数据丢失防护系统（DLP）政策。它通常是机构按照自己的政策和地方/区域法制定的战略和软件的结合。机构要保护信息，有效的DLP是必要的，因为它涵盖了大多数类型的信息丢失，无论它们是有意、无意（人为错误、错位）或犯罪（盗窃、黑客、机构未经信息当事人同意向第三方销售信息）。

（一）DLP如何协助保护数据

大多数DLP政策会根据资料的状态用特定的软件和方法，通过检测和监测三种主要类型的信息，来实现信息保护。

第一类是传输中的信息（Data in Transit）。它包括进、出或流通于组织内部数位化平台的信息。特定的软件会被整合到机构网络去跟踪内部网络的网络运动或任何可疑的网络交通。通过使用深度包检测(DPI)技术，能够选择性地扫描网络中的信息包内容及它们的源头、目的地和流量。要实现这个功能，传输中的信息应该事先解密或软件有能力去解密，检查后再对其进行加密并传送。如果检测到任何未经授权或不符合机构安全政策的信息传输，DLP软件应能够立即停止有关传送并通知发件人的上级。

第二类是使用中的信息（Data in Use）。这比其他两类信息更加难以监控，因为它包括所有电脑内正在使用的信息。例如将信息复制到一个USB驱动器，将信息发送到打印机，甚至是应用程序之间的信息传输。通过软件代理（Agent）设立的规则，DLP可以保护这些信息，迫使用户遵从并限制他们的权利，其中可能包括防止复制信息时终端机未连接到内部网络或阻止用户试图复制敏感信息到U盘。

第三类是闲置信息（Data at Rest）。此类型通常需要一种名为Crawler的软件在机构的数据库中搜索和定位特定信息及档案类型，无论它们是电脑、储存局域网络还是档案存储的信息。Crawler会打开这些档案，并确定它们所包含的敏感信息，然后评估信息是否被放置在中央管理层事先定下的安全规则水平内一个合适的路径。机密信息，如信用卡信息，将被放在安全的路径中并被加密，以防止任何未经授权的访问或活动。此外机构应该定时创建信息备份，以防止可能的硬件、软件故障，停电事故和自然灾害产生的任何信息损失等。

政策方面应设立拥有系统许可权的特权用户，以确保只有选定的个人才可以改变机构的DLP解决方案的设定。最理想的人选就是中央管理层，因为他们更了解日常业务中传输敏感信息的必要性，并对相关政策提出更改，而且发生问题时更容易追究责任。为了避免中央管理层的权力过大，机构必须制订相关政策，防止他们在犯下罪行的同时隐瞒犯罪（例如出售客户个人资料）。提高对信息保护的认识，为员工提供培训，也是DLP的一个非常重要的部分，由于大多数信息丢失事件的发生是由于人为错误，给予他们相关知识亦能减少此等错误和信息损失。

（二）实施DLP解决方案的优点

通过实施有效的DLP解决方案，机构对本地/区域规则和法规的遵守将得到改善，可减少违法和面临诉讼的可能。DLP的另一个好处是，在检讨和测试当前的业务流程中，任何不必要或错误的过程均会被发现。促使中央管理层制订一个解决方案，从而进一步降低安全性漏洞的产生，更好地保护敏感信息，避免任何不必要的信息丢失或泄漏。再者，通过浏览机构的储存服务器和网络带宽，DLP可以识别任何不必要的信息，删除它们并降低备份所需的大小，从而优化磁盘空间和带宽。

（三）实施DLP解决方案要考虑的要点

首先，DLP不是万能的，它有它的限制。例如，无法全面解读所有格式的档案内容，图片上的敏感信息或设计档案可能不能被全面侦查及拦阻；移动设备也较难被监测和控制，因为它们有能力发送短信，拍下照片并录制影像档案。因此随着软件的使用，机构必须制定相应的规则和法规，以提高员工对保护信息安全的重要性和损失信息的严重后果的认识。正确运用适当的规则、法规与软件，能进一步将信息丢失的风险降到最低。

由于DLP软件主要是通过制订规则去执行相应的职责，决策规则过于严格或宽松都将使DLP解决方案的效用降低。若没有正确实施机构的解决方案所需的合适的规则，DLP也可能会带来业务操作上的风险。例如传输中的敏感信息未被成功侦查或其他非敏感信息被过度拦阻。为了尽量减少此类风险，机构的管理层必须制订有关的DLP信息保护规则和业务流程，并在需要时雇用专家顾问协助。通过制订并实施有关的规则和业务流程，以实现信息保护的最佳实践。

个人信息保护立法及监管要求

何晓明 副总监

王 婧 经理

德勤北京事务所
企业风险管理服务

伴随着中国经济的飞速发展和科技的巨大进步，信息时代真正地来到每个人的身边，信息的含金量及其对日常生活的影响日益彰显，为提供定制化的客户服务以提高客户服务满意度，客户的身份、家庭、财务状况等个人信息成为服务提供者需要掌握的基本信息，客户在享受服务提供者提供的量身定制服务的同时，也逐渐注意到，一些推销和诈骗电话对自己的信息了如指掌。此外，由于个人信息泄露导致的信用卡盗用事件的相关报道也不绝于耳，甚至不乏一些人身安全事件。如此诸般，立法机关、行业主管部门、社会媒体等各方力量，越来越多地提到个人信息保护的重要性，也催生了一系列法规及指引的出台。中央电视台2013年3.15晚会曝光的安卓系统第三方应用开发者在未经用户授权的情况下对用户个人信息进行采集，收集了大量用户个人信息的事件，实际上只是以个人移动通信终端为触点，揭示了当前媒体、公众以及个人用户等各方对于个人信息保护的日益关注，事实上，中国政府和监管机构对于个人信息保护监督力度也在逐步加强。

准，也已于2013年2月1日起正式发布实施。此文件属国家标准“指导性技术文件”类，与从制度上进行监管的《决定》相比，该《指南》侧重于从技术手段、信息系统上进行监管，对利用信息系统处理个人信息的活动起指导和规范作用，目的是为了提高企业的个人信息保护技术水平，促进个人信息的合理利用。

除此之外，在《决定》出台以后，各部委也开始制定更具体的个人信息保护的相关规定。工业和信息化部起草了《电信和互联网用户个人信息保护规定(征求意见稿)》、《电话用户真实身份信息登记规定(征求意见稿)》(以下简称《规定》)，并且已经向社会公开征求意见。根据《规定》，电信业务经营者、管理机构及工作人员不得出售或者非法向他人提供电话用户真实身份信息，否则可以处1万元以上3万元以下罚款，构成犯罪的，依法追究刑事责任。

电信行业《规定》的迅速出台，表现了工信部对于个人信息保护的坚决态度和长期以来的渴望。随着电信行业打响了个人信息保护的“第一枪”，我们有理由相信，其他拥有大量用户信息的行业，也将逐步打响保卫个人信息之战。

国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。

——《全国人民代表大会常务委员会关于加强网络信息保护的决定》
(以下简称《决定》)

一、国家关于个人信息保护的立法

2012年12月28日第十一届全国人民代表大会常务委员第三十次会议审议通过的这一决定，为加强公民个人信息保护、维护网络信息安全提供了法律依据。为配合《决定》的落实，在具体的指南方面，《信息安全技术公共及商用服务信息系统个人信息保护指南》(以下简称《指南》)作为我国首个人信息保护国家标

二、个人信息保护的需求及《指南》概述

造成个人信息泄露有多种因素。首先，随着网络的进一步发展，个人信息的价值越来越高。巨大的利益驱动，使得不法分子铤而走险。然而，中国公众目前对个人信息的保护意识不强，给犯罪分子留下了可乘之机。并且我国一直以来缺乏明确的法律法规，对个人信息的收集和使用到底怎样是合法，怎样是不合法并没有明确的定义。同时，对于明显的个人信息非授权收集或流转，也没有足够的惩处力度以震慑此种行为。总体来看，在个人信息处理流程中，个人信息非授权采集和个人信息第三方流转是个人信息保护的两个主要风险点。《指南》分五个章节，分别描述了个人信息保护的范围、参与对象和相关方的定义、角色和职责以及信息处理阶段的具体标准。在该《指南》中对个人信息的类别、信息相关方的类别和信息处理的环节都进行了明确的区别和划分。

(一) 个人信息

《指南》最显著的特点是将个人信息分为个人一般信息和个人敏感信息，并提出默许同意和明示同意的概念。对于个人一般信息的处理可以建立在默许同意的基础上，只要个人信息主体没有明确表示反对，便可收集和利用。对于个人敏感信息，则需要建立在明示同意的基础上，在收集和利用之前，必须首先获得个人信息主体明确的授权。

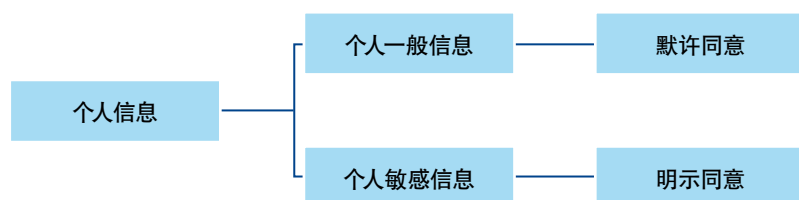


图1 个人信息的分类

(二) 信息相关方

《指南》将信息相关方分为个人信息主体、个人信息管理者、个人信息获得者和第三方测评机构。

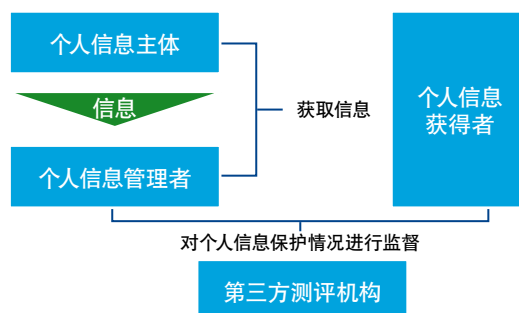


图2 信息相关方

- (1) 个人信息主体。个人信息指向的自然人，信息的真正所有者。
- (2) 个人信息管理者。决定个人信息处理的目的和方式，实际控制个人信息并利用信息系统处理个人信息的组织和机构。

- (3) 个人信息获得者。从信息系统获取个人信息的个人、组织和机构，依据个人信息主体的意愿对获得的个人信息进行处理。
- (4) 第三方测评机构。独立于个人信息管理者的专业测评机构。

(三) 信息处理

《指南》将个人信息处理分为收集、加工、转移和删除四个主要环节，对个人信息保护贯穿四个环节中。

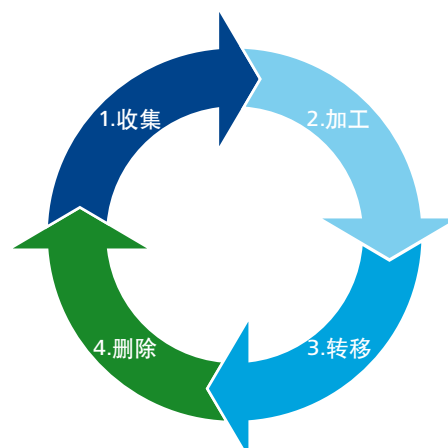


图3 个人信息处理的主要环节

- (1) 在收集阶段，要求目的合法且告知个人信息主体。
- (2) 在加工阶段，要求将加工目的及方法等告知个人信息主体。
- (3) 在转移阶段，要求告知个人信息主体转移的范围和目的。
- (4) 在删除阶段，要求收集阶段告知的个人信息使用目的达到后，立即删除个人信息。

从以上四个环节的要求来看，《指南》主要强调的是个人信息主体的“知情权”，要求对于个人信息处理全部要告知个人信息主体，且处理不能超出告知范围。这项标准还提出了处理个人信息时应遵循的八项基本原则，即目的明确、最少够用、公开告知、个人同意、质量保证、安全保障、诚信履行和责任明确。

该《指南》为下一步有针对性地打击相关犯罪提供了有力武器。但是，这个《指南》仅是一个技术性标准，缺乏对违反这个标准的惩罚性措施，因此对于打击个人信息犯罪尚不具有威慑性。在网络上保护公民权益免受非法侵害、保障国家安全是一项系统工程，不是单靠一部法律、法规就可以完成的。制定具有可操作性的法律必不可少，但要想从根本上解决个人信息泄露的问题，还需要不断完善相关的网络法律法规，建立健全相应的配套制度。

总体来看，我国在个人信息保护立法方面还处于初级阶段，虽然出台了标准并准备颁布法案，但具体法案的实施，细则的补充以及实施还需很长一段时间。

三、个人信息保护主要风险点的应对

结合我国国情，目前应对个人信息保护风险，主要需要国家完善立法、民众提高个人信息保护意识和企业规范信息使用三方面的努力。

（一）在国家立法层面，逐步完善国家立法，尤其是加大个人信息相关违法行为的惩处力度，是应对个人信息第三方流转的有效手段之一

其主要目的是提高相关违法行为的犯罪成本，从而对违法人员起到震慑作用，减少此类行为的发生。我国目前各地政府已开始纷纷“试水”，用实际行动立法保护个人信息，如湖北、湖南、江苏等一些地区，对非法泄露、复制及倒卖个人信息的非法者，处以最高50万元的罚款。随着《决定》和《指南》及一系列具体措施的颁布，对个人信息相关违法行为的惩处力度及范围与日俱增，构成犯罪的，也将依法追究刑事责任。

（二）在公众防范层面，为防范个人信息的非授权采集，需要提高用户的自我保护意识

作为信息的所有者，个人应采取措施对自己的信息进行保护，包括了解个人信息的范围、个人信息保护的原则和可采用的具体措施。姓名、身份证号、电话号码、住址、账号等可以定位到个人的信息都属于个人信息的范畴。

个人在向外界提供个人信息时，应了解对方获取此类信息的原因，并据此判断对方要求取得的信息是否多于实际需要的信息。坚持“最小够用”的原则，只给对方提供必要的信息，避免在不正规的网站、电商留下个人信息。

在提供信息时，应采取措施限定或表明此类信息使用的范围。例如，在提供身份证复印件时，应在不影响复印件使用的情况下，注明该身份证复印件的用途或授权使用人；在网站注册输入信息时，应关注网站是否提供隐私保护政策，限定信息保密要求或限定使用范围。

在处理包含个人信息的介质时，应采取恰当措施销毁信息。常见的信息介质包括：个人简历、快递单、银行业务凭条、刷卡记录等，在弃置此类介质前应保证个人信息不会被获取，可以采用撕毁、涂画等方式保护个人信息。

除个人要加强信息保护外，政府在加强立法保护的同时，还应加大对个人信息保护的宣传力度，借助广播、电视等多媒体，营造良好的舆论氛围，提高全民的信息安全意识。同时，建立个人信息保护制度的奖励机制，鼓励公众举报侵犯个人信息的违法行为，以便从源头上找到真正的元凶。

（三）在企业层面，出于控制声誉风险和法律风险的角度，企业需加强对个人信息的保护

随着立法和监管力度的加强，企业也需要加强对于个人信息保护的关注，严格遵守与个人信息相关的合规要求，包括信息收集及使用规范、安全保障措施和监督及检查等方面，并接受与配合相关机构的监督与检查，尽量避免由于个人信息相关违法行为导致的法律责任追究。

同时，从企业声誉风险的角度来看，客户群体对自身信息保护的意识和重视程度都在逐步提升，众多信息泄露事件的曝光和各类传媒对此类事件的持续关注，都对企业声誉风险的控制形成了越来越大的压力。出于对客户群体的负责，以及自身品牌的维护，企业都有必要加强对个人信息的保护力度。

企业在使用用户信息时应关注用户信息泄露的两个主要途径，包括内部泄露和外部泄露。

- （1）内部泄露。主要有员工泄露（例如2012年3.15晚会有相关报道，系统管理人员批量出卖用户数据）和非法外来人员泄露（例如商业间谍等）。
- （2）外部泄露。主要途径是在和第三方合作的过程中，用户信息在企业不知情的情况下被第三方获取（例如信用卡短信提醒功能的短信平台提供商，存储银行的用户手机号码）。



由于用户信息收集、加工、转移和弃置的过程中都存在信息泄露的风险，因此企业应建立全流程、多层次的用户信息保护体系，因为：

- (1) 一个完整的用户信息保护体系，可以覆盖可能存储信息的管理对象、信息使用管理的全流程，以及信息保护的相关方。
- (2) 一个合理的用户信息保护体系，可以兼顾职责分工、管理流程和技术平台，保证执行人、工作内容和操作工具的高度一致。
- (3) 一个灵活的用户信息保护体系，可以通过对每个局部领域的深入和细化，制订可落地实施的管控措施。

企业在个人信息保护中应全面考虑信息收集、加工、转移和删除环节的风险，应梳理个人信息在本企业使用过程中的全部流程，包括涉及的系统和外包商、合作伙伴，逐一评估流程环节中个人信息泄露的安全风险、客户通知的合规风险、事件处理的声誉风险等。

企业在收集、使用个人信息时，应至少做到：

- (1) 小范围、先认可。在收集环节，只收集必要的个人信息，并根据个人信息的性质，获得信息主体的认可。
- (2) 防泄漏、透明化。在加工环节，采取必要措施防止数据泄露，并向信息主体告知加工目的和方法。
- (3) 不放松、广告知。在转移环节，对外包商和合作伙伴应要求采取与企业自身管理一样的安全管理要求，保证在个人信息使用的过程中不出现管理的短板，并明确告知信息主体转移的范围和目的。
- (4) 及时删、不保留。在删除环节，当使用目的达成后，及时删除个人信息，包括企业自身保存的，以及外包商和合作伙伴保存的数据。

综上所述，企业在管理个人信息时，除做好自身安全管理，关注外包商和合作伙伴的安全水平之外，还要体现对信息主体的尊重和负责，保障信息主体对个人信息使用情况的知情权。

个人资料保护制度建置项目经验谈

吴佳翰 合伙人
曾 韵 高级经理
游靖芬 副经理
德勤台北事务所
企业风险管理服务

许多机构初次听到有新版《个人资料保护法》时，都会问：“我们还要多做什么？”了解法规的内容以后，不禁哀鸿遍野：“这太严格了！对我们的业务执行将造成很大影响！”而那些以往未曾被《电脑处理个人资料保护法》规范的行业，更是惊恐：“罚则这么严？到底应该怎么做才不会被罚？我们连从何开始执行的头绪都没有！”这些冲击都始于2011年5月26日正式公布新版《个人资料保护法》之时，全台湾不管是公务机构或非公务机构都开始“疯”行个人资料保护，并被深深地困扰着。

新版《个人资料保护法》参考APEC隐私保护纲领，各行各业都将受到新规范的影响，即便是过往已遵循《电脑处理个人资料保护法》的产业，其遵循程度仍不够彻底。综观亚太其他地

区（如中国香港、日本与韩国等），其个人资料保护的法令进程与个人资料保护意识均较台湾成熟，对于台湾即将面临的个人资料保护的挑战，或可作为借鉴参考。

德勤在研究了台湾与各地的个人资料保护相关法令法规以及国际标准要求，并融合各产业的个人资料项目经验后，对于个人资料保护机制提出“五个方面与七个步骤”，作为执行个人资料保护的参考。五个方面是：①组织本身；②委托机构；③当事人权利；④预防机制；⑤事后应变（见图1）。七个步骤是：①制订法令基准；②盘点个人资料；③了解风险程度；④设计管理机制；⑤确实遵循机制；⑥进行机制核查；⑦持续矫正预防（见图2）。

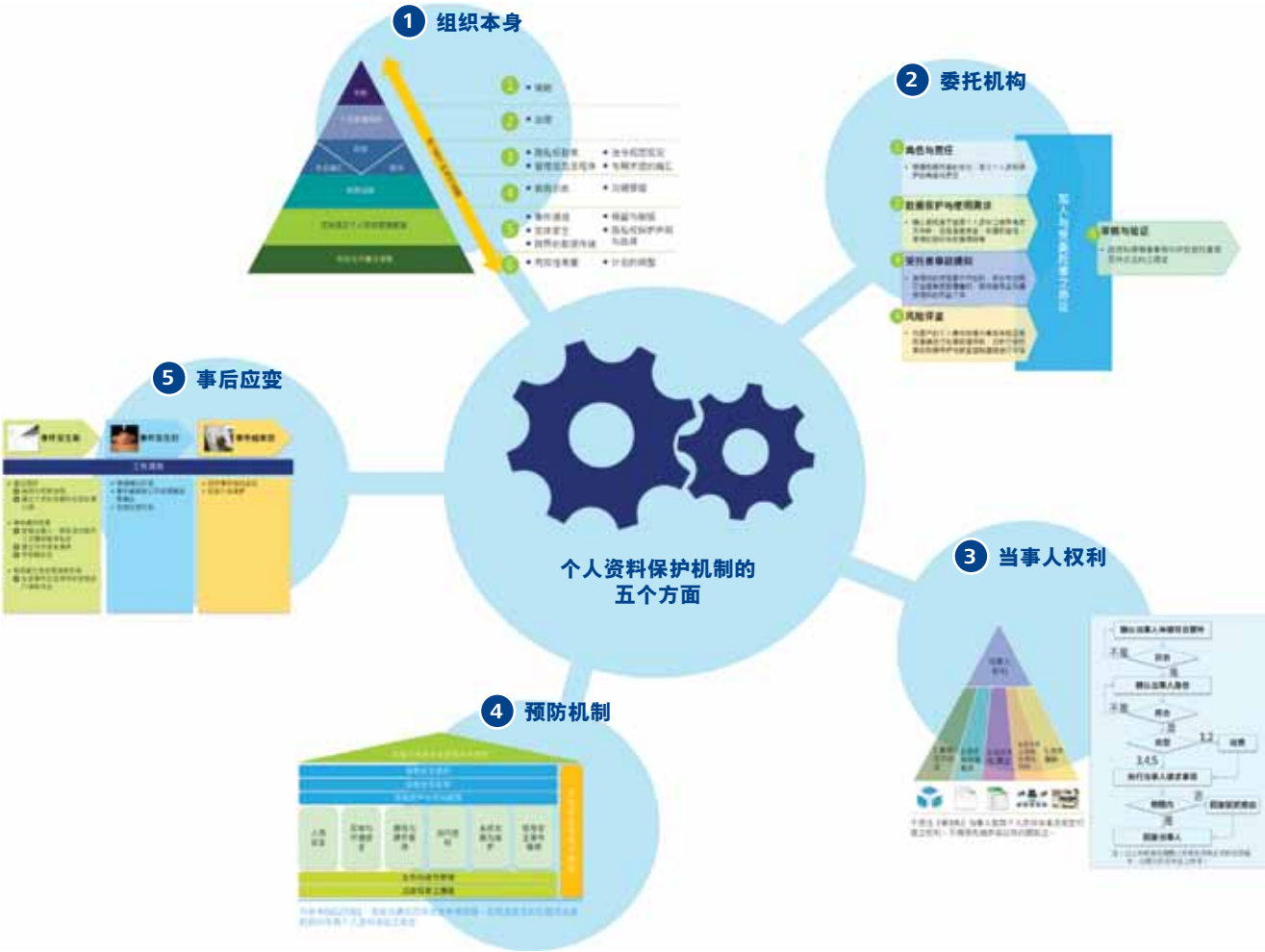


图1 个人资料保护机制的五个方面



图2 个人资料保护机制的七个步骤

各产业因其特性不同，对于新版《个人资料保护法》的规范的确会有窒碍难行之处，以下提出各产业可能面临的冲击。

金融业以往有许多间接搜集个人资料的情况(如信用卡申请书上除申请人的资料外还有其他联络人的信息)，若都要在《个人资料保护法》实行后一年内完成告知，则告知将耗费巨额成本。此外，若考虑删除此间接搜集的个人资料，部分以特殊形式存在的个人资料(如图像文件)则难以完全辨识与删除。

无实体店面的产业在搜集个人资料时以网页形式达成契约关系，并在网页中进行告知作业，但如遇特定目的外的利用时，《个人资料保护法》又规定必须获得当事人的书面同意，故业者往往需要以实体信件寄给当事人以获得同意，或是建立一套符合数字签名原则的身份认证机制，而这皆需耗费高额成本。

以上的两个例子仅是冰山一角，新版《个人资料保护法》已取消行业的限制，各行各业均会受到冲击，在遵法的议题中，不管法律制定的宽松程度如何，法令遵循与业务收益之间的冲突是难解的议题。

在企业进行个人资料保护的作业时，还有另一个难解之题，即个人资料保护的治理架构。在台湾《电脑处理个人资料保护法》的时代，个人资料保护的议题理所当然被认为属于资讯部

门，然而新版《个人资料保护法》公布后，此议题将涉及企业内所有可能接触到个人资料的部门，基本上就是企业内的所有部门。如何把负责个人资料保护作业的权责拓展至各部门，并找出一个主持大局，统筹各部门的人或组织来推动个人资料保护亦是一门学问。只要企业的个人资料保护角色权责能够明确，推行个人资料保护即会事半功倍，并一路顺畅。

若企业了解了法令，明确了个人资料保护的组织，接下来面临的问题就是找出个人资料。大部分企业的问题在于不能明确地辨别哪些是个人资料，或存在个人资料遗漏的不安全感，这些问题都是因为个人档案会在组织内流动而非静止，各部门若是各自盘点个人资料，势必会有漏缺的情况。盘点个人资料，除了须花费时间、人力资源外，盘点的方法也非常重要，好的方法可以让盘点过程更完整、更顺利。

虽说个人资料保护是合规的议题，但信息安全的部分亦不容忽略。举例来说，个人资料进行传输时，为了保护其机密性，可以将其压缩并加密，再用电子邮件进行传输；而以电子文件形式存在的个人资料在删除时，为了使其消失不复存在，可以使用Shift+Del进行删除。但上述的两个案例都不是绝对的，对于安全控管的议题，并没有标准答案。所以企业常会问：“要买什么产品才可以达到保护个人资料的目标？”、“这样的保护程度就足够了吗？”企业常会质疑，科技产品日新月异，到底要使用何种新颖的防护设备才能防止个人资料受侵害，而旧的产品是否都要淘汰？如果盲目地追逐新技术，则企业要付出的成本将永无止境，但不这样做，合规的风险又会很高。建议企业应落实个人资料管理风险分析与评估作业，在设计控管与资源提供时，必须彻底了解自身情况，理性地找到平衡点。

最后，所有的企业都会问一个问题：“实施了所有的个人资料保护措施，个人资料就不会外泄了吗？”或者是进一步问：“如果都做了，个人资料外泄时还会被罚吗？”最终的答案都是：“这要看法官的心证”。基于《个人资料保护法》的概念，如果能证明企业是无故意无过失，即无需被罚。只是企业要完全证明其无过失责任，以法律观点而论较难以达成，只要发生个人资料外泄，势必还是会被罚，只是做得好，罚得会比较轻。处理得当，可以提升客户对企业的信赖感，亦可提升企业形象，进而创造价值。

个人资料保护的实践只是企业经营过程中的一段插曲，过程中的风险从来不会消失，企业必须在风险中寻找创造价值的能力。

个人信息保护趋势浅谈

梁剑凌 副总监

德勤广州事务所
企业风险管理服务

信息和通信网络的持续发展让信息交流和传递变得方便而迅速，存储设备的发展亦令海量数据的存储和携带变得非常容易。人们在享受信息技术和网络的发展带来的高效和便利的同时，也时时担忧个人信息的丢失和泄漏。同时，随着全球化业务的持续发展，个人信息保护也成为国际业务交流中一项重要指标条件。近年来，频繁发生的个人信息泄漏恶性事件更是将个人信息保护推向了风口浪尖，社会对个人信息保护的关注进入到一个新的高度。

2013年3月，云计算笔记应用Evernote向近5000万用户发出重置密码的通知。Evernote表示，近期遭遇了黑客攻击，导致大量用户名、电子邮件地址和加密密码泄漏。¹ 2013年3月，有消息称支付宝转账信息能够被搜索引擎抓取，致使大量用户个人信息泄漏。² 2013年2月，据新闻报道，中国人寿80万份保单信息可在众宜风险管理网任意查询，随后中国人寿发出公告证实消息属实并指出此事故是相关网站升级操作失误所致。³ 2013年4月，北京警方通报称，近期连续破获两个有组织的侵害公民个人信息的犯罪团伙，抓获92名犯罪嫌疑人，在其中一起案件中，多名保险公司工作人员先后出售20余万条客户信息，被诈骗团伙利用后骗得300余万元。⁴

个人信息泄漏，特别是带有商业价值的个人敏感信息泄漏并遭挪用会给企业造成巨大的经济损失，给相关个人带来精神及名誉伤害。美国FBI于2005年进行的一项调查显示，个人敏感信息泄漏事件的平均损失高达16.7万美元。次年8月，美国司法部的一项研究更是将这一数字提高到150万美元。另外，根据美国市场研究机构Ponemon的一项研究显示，每条泄漏记录的平均损失为86美元，而这些数据的机会成本更是高达每条记录98美元。一家曾发生过数据泄漏事件的美国保险公司更公开表示，其在一次数据泄漏事件中的总损失高达410万美元，平均每条记录损失15美元。

国际著名研究公司Forrester在2007年调查了28家曾发生过数据泄漏事件的公司，其中过半的受访者将数据泄漏后的安全与审计策略的调整成本列为首要损失；而43%的受访者将数据泄漏事件后的客户通知、市场与安全反应以及商业机会损失的成本列为首要损失；同时，39%的受访者称遭受了显著的声誉损失，而25%的受访者称将面临司法处分。⁵

信息泄漏事件的频发及其造成影响的日益严重，人们对自身个人信息的保护意识日益加强，如何有效管理个人信息以及全面保障个人信息免受非法侵害已经成为了国内外热门话题。

有关个人信息保护的原则最重要的是经济合作与发展组织（Organization for Economic Co-operation and Development, OECD）在1980年颁布的《关于保护隐私和个人数据跨国流通指导原则》中有关个人信息保护的8项原则，⁶概括为开放性、个人参与、责任、使用限制、数据质量、收集限制、特殊目的与安全（见表1）。

¹ Evernote遭黑客攻击：要求近5千万用户重置密码 中国信息产业网http://www.cnii.com.cn/internetnews/2013-03/03/content_1101342.htm

² 两千支付宝转账信息被谷歌抓取 引发隐私泄露恐慌 新华网新闻http://news.xinhuanet.com/2013-03/29/c_124519198.htm

³ 中国人寿80万份保单泄露客户数据“裸奔”，腾讯网新闻http://qd.qq.com/a/20130228/000296_3.htm

⁴ 新规加大个人信息贩卖处罚：直击非法交易源头 新浪网新闻<http://tech.sina.com.cn/t/2013-04-17/10318248454.shtml>

⁵ Khalid Kark. Calculating The Cost Of A Security Breach. Forrester Research Magazine (April 10, 2007).

⁶ 经济合作与发展组织：《关于保护隐私和个人数据跨国流通指导原则》

表1 个人信息保护的8项原则

年份	监管要求
公开原则	必须以方便的方法和人们容易理解的语言向社会公开有关个人信息保护的政策
个人参与原则	信息主体有权知道自身信息的所在位置，有权对自身信息提出质疑，有权对自身信息进行修改、完善、补充和删除
责任原则	个人信息的管理者对个人信息的保管负全责
使用限制原则	对个人信息资料的提供不得超出收集目的，不得随意提供给第三者
数据质量原则	个人信息必须在利用目的范围内保持正确、完整及最新状态
收集限制原则	个人信息的收集必须采取合理合法的手段，必须征得信息主体的同意
目的明确原则	个人信息收集目的要明确化，不能超范围利用
安全保障原则	对个人信息的丢失、不当接触、破坏、利用、修改、公开等风险必须采取合理的安全保护措施

资料来源：经济合作与发展组织。

许多国家以此8项核心原则为依据制定本国的个人信息保护法，并在此基础上不断进行补充和完善。早在1995年，欧盟就出台了涵盖广泛并极具前瞻性的《个人数据保护指令》。1998年6月，美国电子工业协会、美国工商协会和AOL、AT&T、IBM、Bank of America等100多家主要团体和企业成立了在线隐私联盟（Online Privacy Alliances, OPA），发布了《在线隐私指导》。中国台湾地区于1995年出台了《电脑处理个人资料保护法》。次年中国香港出台《个人资料隐私条例》。在中国大陆，2006年大连市推出针对个人信息保护的地区性规定——《大连软件及信息服务业个人信息保护规范》，而改革开放之先锋的深圳也于2010年提出了个人信息保护的立法起草。在2013年中国两会上，政协委员张近东提交了加快制定《互联网个人信息保护法》的提案。

2012年第2季度，上文提及的国际著名研究公司Forrester发表了《Forrsights Security Survey Q2 2012》，其中对当年个人信息数据泄漏事件进行了调研分析。结果显示，信息数据泄漏的源头分为内部组织和外部合作方，其中绝大部分的信息数据泄漏源自企业内部事件，包括公司资产丢失/被盗、内部人员使用不当、针对公司服务器或用户的外部攻击以及内部人员恶意滥用等。

德勤根据多个行业的调查研究和各种类型项目的经验进一步总结出，组织内部泄密风险存在于整个信息处理过程中。信息处理过程围绕着数据信息的生命周期展开，信息生命周期主要

分为5个阶段（见图1），分别是信息收集、储存、处理、分发和删除，每个阶段都存在潜在的信息泄漏风险。例如，在信息收集过程中，对外包及第三方活动/服务的监督管理存在缺陷或在个人信息的获取过程中发生资料泄漏等都是个人信息泄漏风险。再者，在信息存储方面同样容易出现泄漏风险。信息的储存介质有纸、胶卷、计算机等，在各种介质中储存的信息都有丢失和被窃取的风险。此外，个人信息的使用如果无法确定使用范围及使用目的，使用信息时就可能引起内外部传播、滥用信息等情况，此时就存在极高的泄漏风险。因此，对于个人信息的管理和保护，我们必须站在信息生命周期的宏观角度进行规划，再深入每个具体过程进行分析和把控。

为了进一步完善有效的控制机制，国内外各机构和组织以个人信息生命周期为模型积极制定一系列指引标准来保护隐私。英国标准协会以戴明环PDCA循环模型（P-Plan；D-Do；C-Check；A-Action）为基础建立了有关个人信息保护指引标准BS10012:2009个人信息管理体系(Personal Information Management System, PIMS)，其中第4.7项规定，在收集信息时，收集最低限度的个人信息而不是过多的个人信息；第4.2和4.13项规定，对存储个人信息的设备需加以维护，保证个人信息存储安全；第4.8项规定，确保个人信息仅用于一个或多个指定的目的，而不能为了其他目的对原信息做进一步的处理；第4.14项规定，当个人信息在内外部传输时，要有足够的保障机制保护个人信息等。总体来

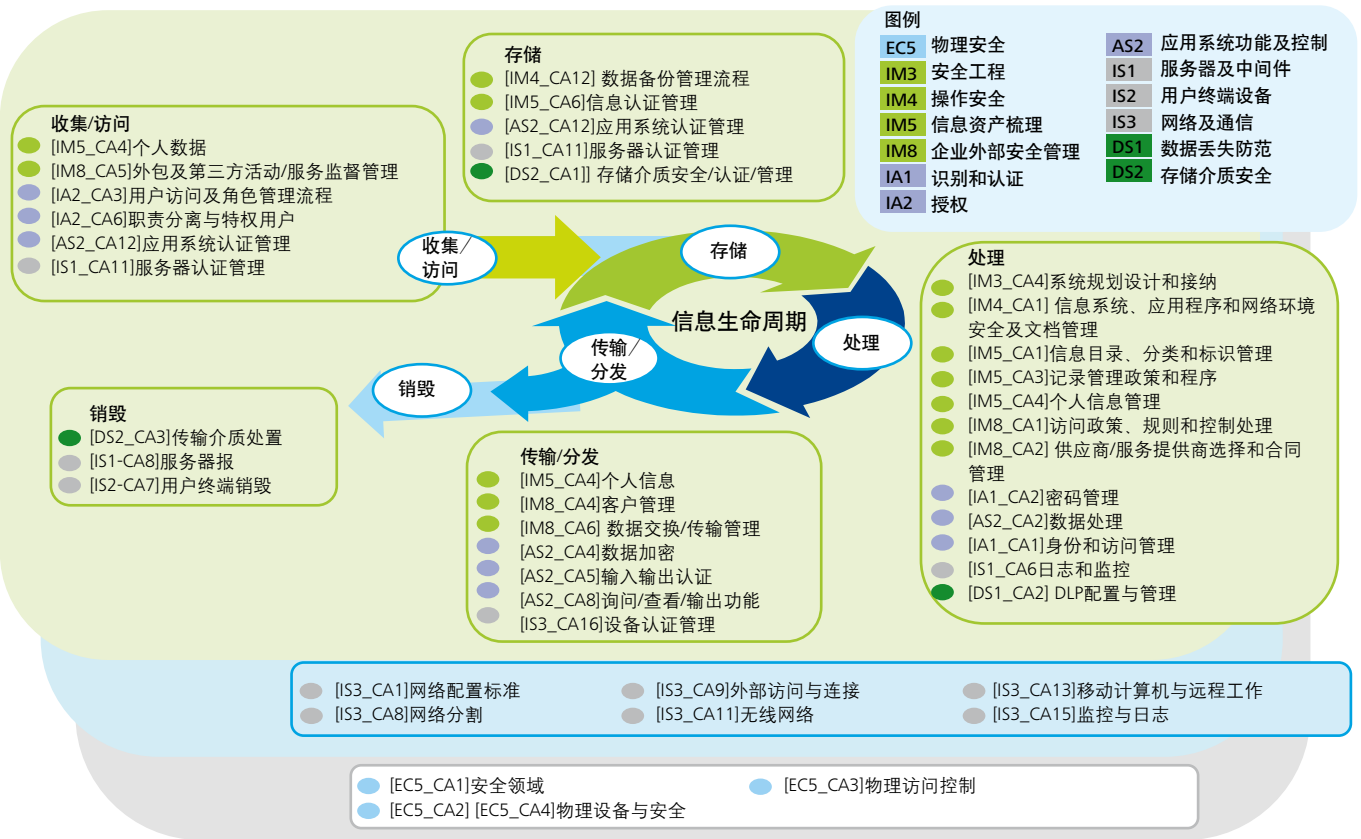


图1 信息生命周期的5个阶段

说，BS10012标准规范几乎覆盖了个人信息生命周期的每一阶段。我国近年来也启动了个人信息保护的相关工作。2012年，国家工信部直属的中国软件测评中心联合30多家单位制定并出台了《信息安全技术、公共及商用服务信息系统个人信息保护指南》，这是我国首个个人信息保护国家标准，于2013年2月1日正式实行。标准对信息系统中的个人信息处理过程的收集、加工、转移、删除阶段进行了规范指引。

个人信息保护的立法正如火如荼地进行着，对于企业而言，建立信息安全机制已迫在眉睫。保护重要的个人信息数据使其免遭泄露，既可避免声誉受损、客户资源的流失以及严厉的司法处分，又利于保持企业在商业社会的有效竞争力。而一旦这些重要数据外泄，将造成企业重要资产的流失。根据国际隐私权专家协会于2012年针对美国、加拿大、欧洲、亚太太平洋等地区的一项调查显示，虽然符合监管机构的法

规要求是信息安全投入的最大动因，但降低风险、保护数据紧随其后，成为第二动因。¹ 他山之石，可以攻玉。随着国内企业跨国业务的快速发展以及企业人员国际视野的日益提高，企业对信息安全的关注重点也将逐步转移到风险管理和数据保护等具体层面。目前我国已有众多企业开始采取积极行动，更加主动地关注数据安全，并将数据分析应用于业务的拓展。国内企业开始意识到保护客户个人信息不单单能够满足客户和业务合作伙伴的期望，提高企业的品牌和公信力，提供有竞争力的差异，更能够减少数据存储成本并增加交叉销售和直销的收入。

数据及个人信息安全保护是科技及互联网不断发展的必然产物。企业通过保护数据及个人信息的安

¹ 国际隐私权专家协会(IAPP). 2012隐私专业人士的角色、职能及薪酬调查.

企业因应个人资料保护的建议

——基于组织、流程、信息科技层面

黄永婷 高级经理

许梅君 经理

李凤仪 副经理

德勤台北事务所
企业风险管理服务

台湾于2011年5月26日正式公布新版《个人资料保护法》，于2012年10月1日正式实施。其法条无缓冲宽限期，且适用对象不再局限于八大民生相关产业。企业未遵循该法将可能产生商誉、法律、诉讼、财务及停业之风险，甚至将会面临高达新台币2亿元的损害赔偿。现代企业经营与个人信息的使用已密不可分，销售、营销企划、人事、客服、信息等部门在日常活动中皆有可能收集、处理及利用个人资料，因此《个人资料保护法》的实施将对各种规模的企业皆造成不小冲击。

多数企业目前已陆续建立并强化其个人资料保护机制，建立个人资料管理组织及程序，并加强相关人员的教育训练。企业面对如此庞大且复杂的个人资料，如何有效地管理个人资料表单及其生命周期流向以及个人资料保护风险，以确保个人资料管理的有效性，并且让组织的个人资料保护措施成为个人资料保护妥善管理的证据，成为亟须解决的议题。本文将从组织、流程及信息科技三个层面对企业提出建议。

一、企业应建立适当的个人资料管理组织

新版《个人资料保护法》及实施细则最主要的改变是加强了企业的责任，包括委外管理、企业内部个人资料保护管理措施、个人资料侵害举证责任等，皆是新版《个人资料保护法》中新增的要求。这些要求同时增加了企业内个人资料保护的相关作业活动，为使其能够在企业内顺利开展，企业应立即建立适当的个人资料管理组织以进行个人资料管理的推行，并确保个人资料保护的观念可传达到每个单位同仁。

目前参考《个人资料保护法》实施细则及相关参考指引，建议个人资料保护组织的必要角色及权责如下。

(一) 个人资料管理部门

依据《个人资料保护法》施行细则第12条及21条，企业内应配备相应的管理人员及资源。同时依据第27条，企业内个人资料保护的具体作业可分成：维护企业内个人资料档案清册、进行个人资料风险评估、制订企业内个人资料保护管理程序、实施个人资料认知倡导及教育训练等。因此，个人资料保护应该是整个企业

的活动而非单一部门的活动，需要有专责人员以企业整体为考虑来规划、带领各部门执行个人资料保护管理活动。例如企业应如何收集全公司个人资料档案清册、应建置哪些个人资料存取管控措施、应如何调整委外契约以符合法规、应如何建立客户收集告知机制、如何留存客户个人资料使用同意记录等议题，往往须通过企业各单位共同讨论，以制订应对方式。目前产业界主要从法务、风管等与法令遵循、风险管控相关的单位中选派合适的人员组成个人资料管理部门。

(二) 个人资料管理召集人及个人资料管理委员会

《个人资料保护法》非常重视企业妥善管理责任的展现，强调企业主的责任，在第50条中要求“若公司个人资料管理不当，公司代表人、管理人或其他有代表权人受相同处罚”。同时，个人资料保护作业因可能直接影响营运方式，在实施前或实施后皆须呈报高阶长官，以确保企业内个人资料保护的方向与目标一致。企业可依其规模大小由第一、二级高阶长官担任召集人及高阶管理团队，并通过定期会议来管理审核作业，以确保个人资料政策的规划执行、资源的有效分配、评估制度的适法性与合宜性，等等。

(三) 个人资料管理代表

个人资料保护的开展除了需要前述两种角色权责外，更重要的是能够在各单位中执行个人资料保护活动的种子人员，这些人员将代表各单位进行相关个人资料管理的沟通协调事宜，确认应遵循的事项。执行项目包含相关业务的推动与执行、个人资料保护的教育培训，并确保各单位可确切落实。

(四) 客户联络窗口

联络窗口主要是作为对客户的联络窗口，因新版《个人资料保护法》中强化了对当事人的告知义务，如第12条要求“若有资料外泄情况，应查明后告知当事人”。因此，依据企业现状，若已有相关机制(如客服、客诉机制)，则可通过既有渠道建立联络窗口机制，以负责接受当事人申诉与咨询；若企业内目前没有类似机制，则至少应建立一个客户联系渠道，为客户提供针对该企业如何使用个人资料的相关咨询。

(五) 稽核小组

为了确认各单位的个人资料管理落实程度、协助发现管控疏漏、厘清疏漏的根本原因，同时协助追踪改善方式，企业可依循内部文化和既有机制来选择适当的个人资料稽核方式，如内部稽核或是单位交叉稽核。

(六) 个人资料侵害紧急应变处理组

疑似个人资料侵害事件发生时，企业须快速因应，掌控侵害事件发生的经过、快速进行调查评估，并于适当时间对内、外有适当响应，因此建议于平日即建立个人资料侵害紧急应变处理组，以因应临时需要的状况。个人资料侵害紧急应变处理组应全面考虑事件管理、调查评估、公关媒体沟通等事宜，以完整涵盖在侵害事件发生时所需进行的事项。

个人资料管理不仅是守法议题，更是企业组织的管理议题，其风险将影响企业的生存与品牌商誉，包含当事人权利展现议题、数据安全管控议题、个人资料风险管理议题、个人资料侵害紧急应变处理议题，这些都需要企业投入适当的资源、人力，并通过跨单位管理来规划、执行并持续改善个人资料保护管理体系。企业可通过上述个人资料管理组织的角色权责来检视内部状况，而个人资料管理组织的重点不在于新增哪些专责人员或专责单位，而是需确认在个人资料保护管理机制运行时各项权责在企业内皆有对应的人员及单位，以真正落实个人资料保护管理。

二、从个人资料生命周期入手调整流程，降低《个人资料保护法》对企业营运的冲击

《个人资料保护法》要求个人资料档案应明确定义，且企业在收集、处理及利用个人资料前，须和当事人进行清楚的告知作业。所取得的个人资料在处理及利用过程中，应实施较一般资料更为严格的管控。同时，当事人依据企业存放的个人资料进行资料复本获取、资料新增、资料查询、资料更正等作业。

反观企业活动，销售、营销企划、人事、客服等部门在其日常活动中皆有可能收集、处理及利用部分个人资料。因此，决定哪些流程需调整，确认调整方向，集中资源进行核心营运活动的调整皆是企业目前最关键的问题。



建议企业梳理个人信息生命周期，辨识个人资料收集、处理及利用活动，找出业务流程差异点。以下将依据《个人资料保护法》的要求分享业界常见的议题及建议。

(一) 个人资料收集、处理及利用要求对营运流程的冲击

出于人权保护，《个人资料保护法》要求企业应让客户了解个人资料收集的目的及个人资料的使用方式，确保资料的使用符合当初客户授权的目的。然而在现行复杂的营运活动中，个人资料在企业间互相传递，企业所持有的可能已是第二手甚至是第三手的资料。企业为开拓客户，通常有多种资料收集渠道，而集团间、企业间相互分享或提供客户名单的状况也时有所闻，导致企业常常难以追溯个人资料最初的收集来源及目的。

1. 分析业务收集目的

企业需先盘点所有的资料收集端，界定企业是直接收集抑或是间接收集的角色，所有的收集活动是否皆符合业务特定目的并已完成收集告知且获得同意。可以从企业的盈利登记来定义个人资料收集目的，但若其目的不在原盈利登记内，是否导致不得收集个人资料，或是过往收集的個人資料不能再利用？然而个人资料在企业内并非为单一业务存在，而是由各类业务需求而产生的一连串信息，因此企业需从业务层面分析个人资料收集的必要性及目的，同时再从个人资料档案支持业务的层面比对个人资料档案与业务的关联，以确保该个人资料档案存在企业的合法性。

2. 界定收集时点判定原则

在新版《个人资料保护法》实施前收集的资料，可能没有收集目的，该法不追溯过往所收集的個人資料及收集活动，但规范现行企业对该个人资料的使用状况，因此在规范要求上出现时间差，以前收集的资料不一定能继续使用，造成营运冲击，因此建议企业应界定个人资料的收集时点判定标准，针对旧有收集的资讯进行标示，若在企业营运活动中需再利用时，需再进行相应的告知及同意活动。

3. 应为各类收集渠道设计收集告知及同意程序

企业除了通过实体渠道收集客户个人资料外，也可利用许多虚拟渠道，通过电话、网页等收集资料，因此需针对不同的收集渠道设计不同的告知、同意方式，以便让收集端同仁方便和

客户说明，收集的個人資料在后续处理及利用过程中可有明确的判断依据，收集的证据可在未来使用。建议企业可从公司层面考虑建立收集告知同意程序及告知范本，先制订一致的特定目的、个人资料利用方式供各业务参考，再由各业务依据业务特性进行差异化。

(二) 个人资料处理、利用管控与业务便利性议题

1. 实施适当的个人资料安全管控措施

《个人资料保护法》第27条规定，针对数据处理、利用要求应实行适当的安全措施，同时实施细则中要求企业加强个人资料保护。在收集、处理及利用活动中建立企业管控程序及安全防护措施，如个人资料的存在最小化、安全储存及销毁的规范、使用及传递的加密保护。不论是管控程序或是防护措施皆可能直接影响业务便利性与效率。企业常陷入安全保护与业务便利性的冲突思维中，然而《个人资料保护法》并非要求企业滴水不漏地保护个人资料，而是要求在企业的管控水平中展现管理责任，因此建议企业可积极地设定个人资料管控策略，从风险评估中选择适当的个人资料管控。

2. 客户拒绝营销机制

《个人资料保护法》规定，企业应向客户提供表示拒绝接受营销的方式，并负担所需的费用。营销作业是企业重要的营运活动，业界存在多样且复杂的共同营销模式，针对渠道分享模式，企业应确保在平面广告或文宣中提供免费客服电话或电邮联系方式。针对从他处取得的会员名单，应在联系时说明收集的资料、来源及使用的目的，同时设计沟通技巧，以取得客户信任，满足客户对个人资料使用的了解需求，并依法提供拒绝渠道。

(三) 当事人权利行使流程

《个人资料保护法》为保护人权，特别强调当事人对其个人资料的权利，并要求企业在一定时间内回应客户的请求。除了既有的资料查询、更正及提供复本的流程外，企业须再提供申请删除及停止收集、处理利用的流程。为清楚界定客户请求删除或停止处理、利用的资料，建议企业向当事人提供权利行使渠道及行使表单，通过前端同仁的说明及申请单内容，预先过滤定义不清或是意图不明的请求。同时对内建立判断原则，便于业务端同仁有一致的处理标准，符合法规的回应时间，同时提供适度合理的处理回复。

(四) 委外管理流程

《个人资料保护法》第4条特别强调受托机构视同委托机构，应受到同样的规范管制，并于实施细则中更严谨地在委外合同签订前、委外作业执行中及委托关系终止时分别要求企业对委外单位进行监控。企业应先界定个人资料业务中与合作单位的关系。然而如今企业间业务往来密切，个人资料档案抛转频繁，难以清楚界定是委外还是合作。建议企业可先通过合作厂商所承揽作业的特定目的来判断是否为企业既有作业的延伸，借以辨识是否为受托机构。与受托机构签订的合同中需要完整包含实施细则中的要求，未来将依据合同实施对应检查作业。而针对其他交换过客户资料的合作单位，则可依据业务特性适度要求该单位出示个人资料保护措施。

(五) 企业个人资料管理流程

个人资料管理不仅仅是个人资料数据安全管理、当事人权利展现议题，还包括资料风险管理议题，个人资料侵害紧急应变处理议题。企业应定期执行个人资料盘点流程，以更新个人资料范围，通过个人资料管控检查确认企业个人资料保护的有效性，并反馈于个人资料风险评鉴，了解个人资料风险变化，以实现个人资料管理持续改善。这些新增的个人资料管理活动可并入原有管理活动中，建议企业在理解个人资料管理意图的基础上，对应内部既有的管理模式，适度地在既有的管理活动中加入个人资料管理议题，以降低新增流程对企业所造成的影响。持续改善的个人资料管理活动需要企业组织的配合，也需要相关解决方案的配合，才可以让企业在个人资料管理上更具效益。

三、以整体风险管理观点实施个人资料保护信息科技解决方案

2012年，德勤与美国《富比世》杂志合作，针对全球192位大型企业高阶主管进行有关企业风险管理的调查，结果显示，超过50%以上的受访企业表示，计划将投资有关持续性风险管理与监控的信息科技解决方案。同时约33%的受访企业表示已经在建置自动化风险管理解决方案。因应《个人资料保护法》实施，近年来谈到个人资料管理科技解决方案，大多会直接联想到相关的安全防护解决方案，例如数据安全防护、加解密或稽核日志管理工具，而上述主要是个人资料控管保护作业层面的应用，若以整体企业风险管理观点出发，个人资料保护信息科技解决方案不仅要考虑风险管理对于企

业价值的保护，也需要考虑企业价值的创造。因此个人资料保护风险管理科技解决方案须由个人资料管理、个人资料安全防护、个人资料事件鉴别调查等三个层面发展实施。

(一) 个人资料管理科技解决方案

有关个人资料管理科技解决方案，可以考虑对管理体系、风险评价以及个人资料数据流与个人资料清册管理等作业优先以科技辅助其运作，其他个人资料管理流程，例如当事人权利行使等流程，则可考虑整合于组织现行的相关业务流程平台实施系统运作。

1. 管理体系

个人资料保护管理机制的导入需要持续有效的运作与改善，因此组织会基于PDCA（Plan-Do-Check-Act）的循环持续运作，并通过核查作业及有效性测量指标的衡量方式，确保个人资料保护机制的有效落实。

现行的核查及矫正预防措施追踪及有效性测量指标往往以纸本及人工方式汇整及管理，借由自动化解决方案，有助于快速掌握查核结果，并实时且便于了解各部门矫正预防措施的执行情形。同时也可通过分析报表，掌握个人资料保护的运作状况，并通过有效性测量指标的统计分析结果，监控测量目标的达成，并作为高阶管理决策判断的基础。

2. 风险评鉴

《个人资料保护法》实施细则规定，安全维护事项中须包括适当的个人资料风险评估及管理机制，借由分析组织可能面临的风险与威胁，确认是否需实施风险降低或风险移转等计划，以作为选择个人资料保护控管措施的依据。

个人资料管理的涵盖范围横跨组织各部门，若个人资料保护风险评估由各部门分别进行，则不易汇整，沟通成本高，且不易从公司层级掌握风险评估结果与风险分布。自动化的解决方案将有助于各部门自行执行风险评估作业，并实时掌握个人资料侵害事件的威胁，帮助管理者整体掌握各部门的风险评估结果与改善状况，进而达到实时风险监控与报告。

3. 个人资料数据流与个人资料清册管理

个人资料管理的首要活动为针对企业个人资料数据流与个人资料窗体进行分析与盘点，依业务流程描述个人资料的流向，清楚直观地辨识出个人资料档案收集、制作、传输、使用等不同生命周期，并以此作为个人资料清册的基础。

然而目前多数组织主要通过人工及档案方式收集与管理个人资料清册信息，这不利于日后更新以及跨窗体与流程查询，通过科技辅助，可以将图像形式的个人资料数据流快速转换为数据表形式的个人资料档案清册，并且通过集中化及网页化方式，让各部门以单笔或批次方式更新及查询个人资料清册数据，以利于个人资料清册数据的维护与管理，确保个人资料清册数据的正确性与完整性。

因此通过个人资料清册自动化解决方案有助于支持当事人行使权利时查询相关窗体的流向与储存地，支持个人资料档案侵害事件处理的相关信息查询以及个人资料窗体的相关保护措施布建情形，并且有助于查询个人资料窗体的新增、异动或删除的历史纪录，以有效监控个人信息管理制度的持续有效营运。

(二) 个人资料安全防护科技解决方案

个人资料生命周期中，收集、储存、处理利用、传输与销毁等阶段皆须配备适当的安全防护措施。组织可通过个人资料管理信息环境科技评估，了解组织安全控管的缺漏，并可通过数据安全防护、数据库内容监控、安全事件管理、传输加密机制及数据库内容加密等技术解决方案，强化个人资料保护安全控管的落实与防护程度。

此外，依据《个人资料保护法》要求的实行举证责任倒置原则，组织应留存有证据能力的记录与稽核日志记录，作为提供无故意与无过失的重要证据，因此组织可借由稽核日志管理自动化解决方案，协助稽核日志的收集、储存、分析与报表制作。

(三) 个人资料事件鉴定调查科技解决方案

当发生个人资料侵害事件时，企业除了需要具有个人资料侵害事件的通报及应变机制外，还应配合《个人资料保护法》留存完整的证据，采集证据的过程亦须符合搜证程序，以提出有证据能力的记录作为善良管理义务证据。

因此在侵害事件的处理与鉴定过程中，需要数字鉴定证据收集工具，包括影像文件制作工具、硬盘复制及写保护工具，系统数据收集工具及数字鉴定分析工具等科技辅助工具，以确保数字证物被妥善保存，同时鉴定结果能成为不可避免诉讼时法庭认可的依据。

四、结语

企业应为个人资料保护管理机制的运行投入相应的资源，以尽善良管理的职责。除了在“组织”与“流程”层面建立个人资料管理组织与管理机制外，亦须考虑“信息科技”层面，以提升个人资料保护机制的落实度与有效性。此外，在引入信息科技解决方案时，除了安全防护解决方案外，更应从企业风险管理的整体观点出发采取各层面的解决方案，以使个人资料保护风险管理作业不仅能够实现企业的价值保护，进而能够实现价值创造。



隐私保护的企业现状和合规挑战

李 扬 经理

德勤北京事务所
企业风险管理服务

连续几年在3.15晚会上曝光的质量问题中，都涉及国内大型企业对客户隐私及信息泄露的话题。2011年的3.15晚会，曝光了电信公司贩卖手机用户信息，引起后续电信运营商对自身安全管理的再一次建设。2012年的3.15晚会，多家银行被曝内部员工出售客户信息，其中包括了国内最大及最知名的几家银行。而2012年曝光的案例中，不仅仅涉及客户信息被出售，更严重的是犯罪者利用购买来的客户信息，逐个尝试登入网银。由于银行出售的个人信息包括诸多隐私数据，致使犯罪者成功利用这些隐私信息登入网银，最终造成3000多万元的损失。

由于我国一直没有针对个人隐私保护的相关法律，所以在个人隐私保护方面，更多是由社会舆论和媒体在推动，企业并没有强制性的合规要求需要满足。因此在实施个人隐私保护方面的动力并不足够。往往是出现敏感信息泄露造成企业损失，或者媒体曝光引发公众舆论和信任危机时，才会弥补式地加强在个人隐私和敏感信息方面的保护措施。

事实上，由于移动互联技术的快速发展，企业面临的隐私保护问题日益严峻。据不完全统计，每400封电子邮件中，就有一封包含敏感信息。每2个U盘中，就有一个包含有敏感信息。在网络通信及移动介质被频繁使用，且没有建立敏感信息保护体系以及综合应用信息防泄露产品结合加密机制的情况下，很难防止隐私数据和敏感信息的泄露。

从行业来看，通常以下这些类型的行业需要关注个人隐私及敏感信息的保护：

(1) 金融行业。银行、保险和证券公司为了进行正常的金融交易，均需要收集大量的个人信息。其中银行涉及信贷及信用卡开办的业务，需要更为详细、真实的个人资料。而投保的过程中，个人住址、家庭信息等均会被保险公司收集。这些信息涉及大量的个人隐私，一旦被泄露，信息主体就会被骚扰。而相关的银行账户等也面临被恶意者利用隐私数据入侵的风险。

(2) 医疗行业。医院、卫生所、医疗设备维护机构等，在工作过程中均涉及的大量个人健康状况，是非常敏感的个人隐私信息。早在2008年，深圳市就有泄密光盘兜售十万孕产妇信息，一张光盘售价1.2万元，内容涉及深圳70余家医院。而在2013年被曝光的某医院妇产科护士，在接生后即通过电话给多家机构和个人贩卖婴儿家庭信息，获利颇丰。

(3) 具有自主知识产权的制造及半导体等行业。发动机、半导体芯片等的研发往往需要3~4年的时间，其中涉及大量的专业人员、设备和其他资源的投入。而现在的设计图纸均以电子文档方式保存，极易被泄露。一旦被竞争对手获知，所造成的损失将难以估量。

这些行业涉及大量的个人隐私和敏感的商业信息，但在实施保护措施方面面临着诸多挑战，阻碍了这些企业建立敏感信息保护机制。具体而言，这些挑战主要有：

(1) 缺乏适当的法规、行业标准和最佳实践可以遵从。在2012年之前，我国还未颁布针对个人隐私保护的可执行的法规，并且没有明确的行业监管要求强制涉及个人隐私的特定行业对个人隐私采取适当措施进行保护。在美国，医疗行业的HIPPA法案对于涉及收集个人健康信息的多种行业进行了严格限制，并且在违反法案时会有极其严厉的处罚。在美国、欧洲、日本、中国香港及台湾，均颁布执行了与个人隐私保护相关的法律，在所辖范围内严格执行。

- (2) 难以识别和管理企业内部的敏感信息。个人隐私和敏感信息会贯穿整个业务过程，涉及多个部门及岗位。而对于这些敏感信息的管理责任缺乏明确界定，是企业目前普遍存在的情况。很多时候，在进行这些信息的保护工作时，企业自然而然将此作为信息技术部门的责任。实际上，业务信息的产生、管理和使用时应当遵循的规则，应当由相应业务部门制订，并承担所有者的职责。信息技术部门仅作为信息的保管者，遵循以上规则，设计技术控制措施，并落实执行。
- (3) 缺乏敏感信息保护方法和工具。从以上第二点可以看出，敏感信息贯穿于企业主要业务过程，涉及的部门和岗位众多。如果无法识别敏感信息的位置和信息泄露的渠道，则难以真正对这些信息进行保护。

虽然个人隐私和敏感信息保护面临以上诸多挑战，但是现在也有不少企业意识到了敏感信息保护的重要性，在逐步加强这方面的管理。在政策层面，2012年12月28日，十一届全国人大常委会第三十次会议审议通过了《关于加强网络信息保护的决定(草案)》（以下简称“草案”）。草案中明确定义了个人隐私信息的保护要求，其中第三条“网络服务提供商和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供”明确了对涉及收集个人电子信息的企事业单位对于保护隐私信息的责任。

在管理和技术方面，现在也有诸多公司提供专门针对敏感信息保护的咨询服务及相应防泄露产品。对于个人隐私及敏感信息的保护，企业可以参考如下步骤对自身业务过程中涉及的个人隐私和敏感信息进行保护：企业首先需要界定需要保护的信息的分类及相应等级，识别这些信息泄露的渠道。基于对信息泄露风险的识别，制订相应的访问控制策略，在信息的使用、处理、存储、传输及销毁各环节，应用策略进行管理。而大量敏感信息在企业各部门的分布和泄露渠道的控制，则需要借助信息防泄露产品及加密技术。



管理数据隐私的利器 ——身份和访问管理

薛梓源 合伙人

王会明 经理

德勤北京事务所
企业风险管理服务

随着信息技术的快速发展与广泛应用，组织发展对信息技术的依赖程度日益加深，信息技术已贯穿于各类组织的运营活动中，信息资源已经成为各类组织发展必不可少的重要生产要素。随之而来的是支撑组织日常运营的应用系统、数据库、操作系统和计算机网络等IT资源日渐庞杂，管理成本逐年增加；并且随着企业IT平台的复杂化和开放化，组织和个人数据的安全管理面临很大的挑战。这些挑战包括但不限于：

- (1) 业务增长迅速，越来越多的系统、设备和应用提供关键业务功能，管理和分配这些IT资源的复杂性逐渐增加。
- (2) 各类用户需要频繁访问不同级别的系统、设备、应用和数据，而分散的身份管理和口令管理给用户带来了极低的访问效率和用户体验。
- (3) 不同类别的用户需要不同的安全访问控制，而当前大多数组织还不具备这个能力。
- (4) 组织人员变动带来更多复杂的安全隐患，包括权限蔓延、冗余身份、弱口令等安全隐患。
- (5) 分散的身份和访问管理给合规性审计带来复杂度。
- (6) 互联网云时代仅仅依赖边界保护已经无法保护组织和个人隐私安全。

因此，企业管理者不仅要面对组织和个人信息隐私的安全保护，还要满足内部和外部的合规要求，而要解决上述挑战，统一的身份和访问管理机制可以作为当下和未来亟待采纳的重要举措。

一、身份和访问管理发展现状

事实上，身份和访问管理（Identity and Access Management, IAM）在国际上并不是一个新概念，身份和访问管理系统在2000年前后就已经在市场上出现，并在随后几年达到了一定的规模。随着IT环境的变化，身份管理带来的问题越来越严重，例如：随着无线网络飞速发展，移动计算和远程访问越来越普遍，信息系统被非授权访问的几率显著增加，而非授权访问带来的组织信息泄露的事件频繁发生。

伴随着这些严峻的挑战，身份管理市场需求快速增长，并逐步形成了稳定、成熟的市场规模。而目前在这个市场上角逐的厂商主要包括CA、IBM、Novell、Oracle、BMC、HP、Microsoft等。

IAM 的应用，不仅能为用户带来更低的管理成本，信息安全风险发生的概率也会随之降低，对法规也有了更好的遵从，并能更快地交付增值的IT服务。而最为重要的是，能为组织实现IT投资价值的最大化。

中国大陆对于身份和访问管理系统的建设起步比较晚，主要是因为国内应用系统的建设相对滞后，总体水平并不高，很多组织还把主要精力放在单个系统的建设上；但是随着组织信息化的深入，信息化建设程度领先的组织开始考虑应用系统集成的问题，而统一的身份和访问管理作为应用系统集成的一项重要内容，也逐渐成为组织IT建设的重点。

二、身份和访问管理总体能力框架

身份和访问管理的核心能力包括身份管理、访问控制、身份开通、身份和策略库四部分。将这些能力通过IT技术集成到一起能够为组织提供一个统一的身份和访问管理的端到端平台。身份和访问管理总体能力框架如图1所示。

（一）身份管理

集中的身份管理解决方案可以完成用户身份信息全生命周期的管理。通过将不同类型用户的授权委托给不同的部门、应用甚至是实施厂商，可以减少管理的成本，提高生产效率。

- 全局用户身份的创建和维护。
- 提供集中的、委托的、自助的或三者相结合的管理模型。
- 支持用户身份信息的分级委托管理将减少与身份管理相关的时间和成本。身份信息的管理可以唯一地指向特定的用户或特定的用户群。
- 自助服务允许用户自行维护个人基本信息、修改个人密码口令、忘记密码口令后自动找回，从而减轻系统管理员的工作量。
- 提供对管理事件的报告和审计。

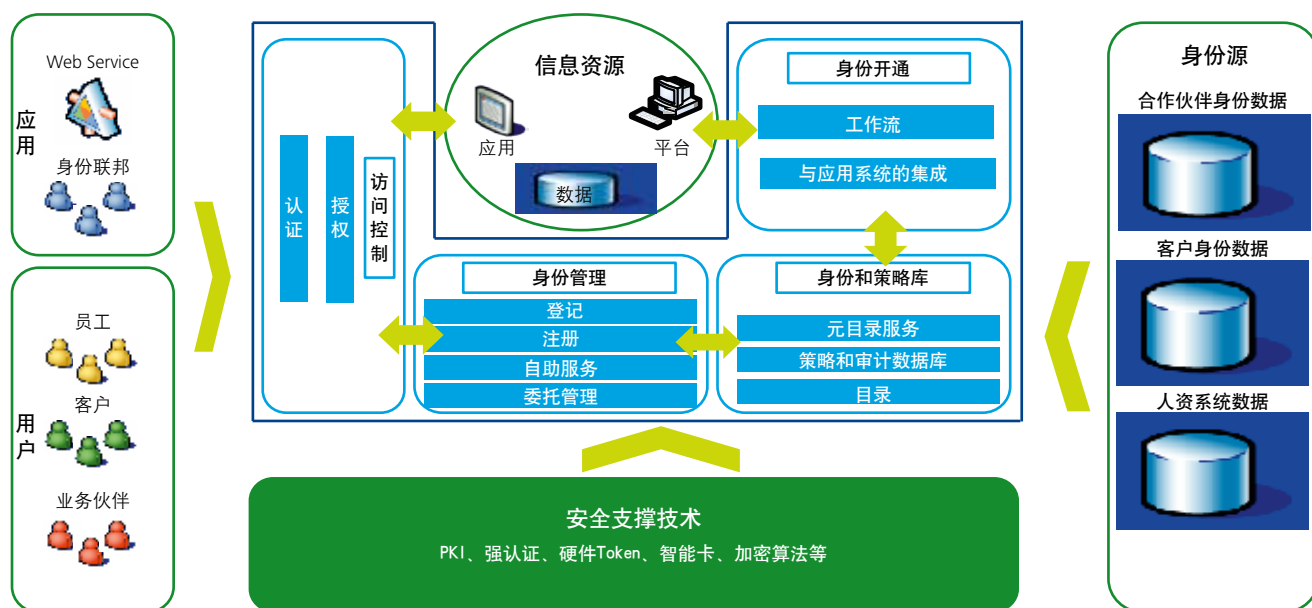


图1 身份和访问管理总体能力框架

(二) 身份开通

身份开通服务按照业务策略和规则，将用户身份从权威账号源传播到目标系统自身的身份库，实现应用账号的集中开通，从而提高了安全性。同时自动化的手段降低了管理成本。集成的工作流提供一种自动化的方式来请求和批准身份管理变更，支持一致的业务规则和流程。

- 迅速、自动地将用户身份从统一的身份库传播到目标资源自身的身份库。
- 替代手工操作，根据集中的策略和业务规则来提供用户的账号开通。
- 集成可定制的审批工作流。
- 通过连接器（个别系统采用API调用）来实现与应用系统的集成。

(三) 访问控制

访问控制提供用户的身份鉴别、安全的会话管理，并为后端受安全保护的资源提供授权服务。访问控制可以通过像Web访问控制和操作系统访问控制等技术来实现。通过提供单点登录的解决方案，减少用户重新登录才能办理业务的复杂性，提高用户的体验。

- 认证服务。认证服务负责对用户身份的真实性进行验证，通过对用户的Session进行安全管理，为用户提供对企业内的应用和资源的无缝访问，且无需重复登录。
- 授权服务。授权服务负责验证用户访问受安全保护资源的权限，验证过程以用户的角色或策略为基础。

(四) 身份和策略库

身份和策略存储提供统一储存用户身份信息、访问规则策略和审计日志信息的功能。是访问控制、开通服务和身份管理服务的基础。

- 权威账号存储。储存用户的全局身份信息、应用身份信息和资源信息。
- 策略数据存储。储存用于身份开通的策略信息和访问规则信息。
- 审计数据存储。储存身份和访问管理所有相关的审计和日志信息。
- 目录服务。能够为支持LDAP和PKI的应用系统提供集中的认证和授权。

三、德勤企业身份和访问管理实施方法

身份和访问管理是一套全面的建立和维护数字身份，并提供有效的、安全的IT资源访问的业务流程和管理手段，通过IAM实现企业信息资产统一的身份认证、授权和身份数据集中管理与审计。德勤的IAM服务能够帮助客户设计、实施、部署和维护集成身份识别和访问管理解决方案。图2为德勤身份和访问管理实施方法涡轮图。

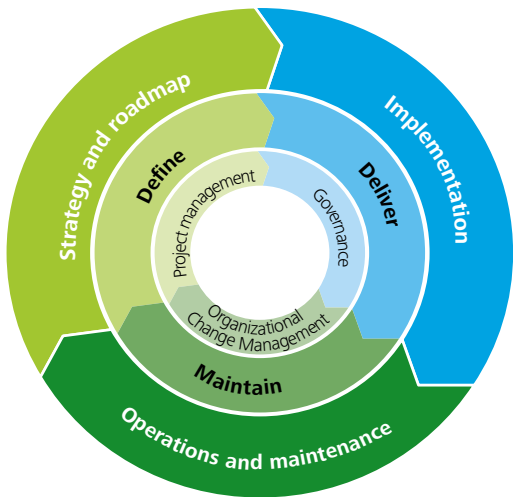


图2 身份和访问管理实施方法涡轮图

从涡轮图我们可以看出，德勤按照战略和路线图制订、实施、运行和维护三个阶段来组织身份和访问管理体系的建设，图3是这三个阶段主要涵盖的工作流。

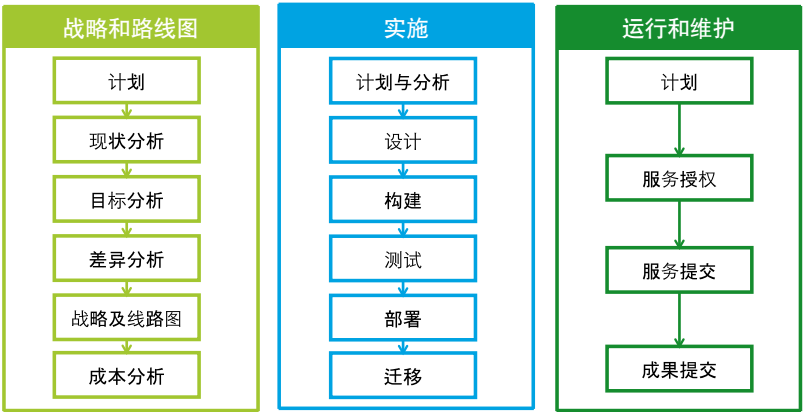


图3 主要工作流

在战略和线路图阶段，组成该阶段工作流的活动如下：

- 计划——确认IAM目标和愿景覆盖的范围。
- 现状分析——了解现状，包括业务挑战、业务流程和现有架构。
- 目标分析——识别短期和中期的IAM服务需求，讨论满足需求所需的业务流程和技术选项。
- 差异分析——实施现状与目标的差异分析，定义IAM的成熟度模型，识别相关技术工具。
- 战略及路线图——创建IAM战略，标识IAM实施的相关时间、优先级，准备IAM项目业务用例。
- 成本分析——确定需求预算和IAM项目的成本分析。

在实施阶段，组成该阶段工作流的活动如下：

- 计划与分析——对实施项目进行计划和分析。
- 设计——进行解决方案架构设计，包括功能模块和非功能模块，以及硬件、软件架构等。
- 构建——根据设计成果，组织系统搭建，编写代码，并根据设计方案进行参数配置。
- 测试——执行系统集成测试、性能测试以及用户测试，验证系统有效性。
- 部署——评估系统的准备程度，执行部署的筹备工作，制订回退策略，将解决方案部署在生产环境并验证部署的有效性。
- 迁移——将构建的系统正式交付使用。

在运行和维护阶段，组成该阶段工作流的活动如下：

- 计划——制订运行和维护服务计划。
- 服务授权——明确身份和访问管理服务执行流程并提交管理层审批。
- 服务提交——根据管理层审批的流程执行服务交付。
- 成果提交——执行知识转移和经验总结，并向管理层沟通和汇报。

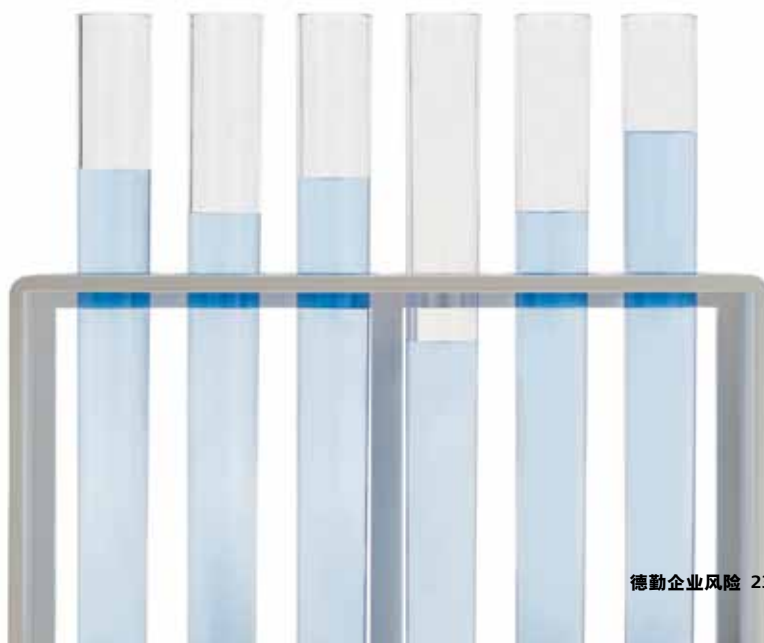
四、身份和访问管理成功要素

身份和访问管理的成功实施依赖于组织的战略目标、核心业务需求和现有应用环境。每个组织的身份和访问管理体系建设都应考虑下述成功因素：

- 管理者需要意识到身份和访问管理的战略性，审慎评估对组织可能带来的影响和转变。
- 明确驱动规则以及身份和访问管理工作流定义的安全策略。
- 实施部门需获得管理层的全力支持，并认可流程改造所带来的影响。
- 关注身份和访问控制管理流程优化改造、人员和组织的转变管理，技术只是身份和访问管理的实现手段。
- 采用基于请求的管理模型来模仿组织现有的权限管理流程。
- 逐步实现基于角色和基于规则的权限授予模型，实现基于请求流程的自动化实现机制。
- 准备全面的转变管理和交流计划。
- 采用分阶段的方式集成目标系统以及支持不同类型用户的身份和访问管理。
- 根据需求分析审慎地进行身份和访问管理软件选型。

五、结束语

今天的组织在身份认证与访问管理方面面临着各种各样的挑战，除了要充分意识到它的重要性和艰巨性，还需要寻求更为自动化且更为安全的身份识别与访问管理解决方案。组织内部和外部的环境变化要求进一步提高管理职能的效率以及管理执行的力度，同时能够尽可能地控制管理成本。组织管理者只有充分意识到身份和访问管理是一项长期的管理工作，而不是一个项目或者一次性的行动，才能在组织内部推动该项管理工作，并借此给企业带来长远的收益，这些收益不仅仅局限于管理效率 and 安全性，更包括长远的战略目标实现和组织声誉。



个人资料泄漏调查经验分享

曾 韵 高级经理

宋子莉 经理

德勤台北事务所
企业风险管理服务

台湾新版《个人资料保护法》已于2012年10月实施，在这部与企业及民众都有切身利害关系的法律实施之后，各产业都无法置身事外。放眼2012年，个人资料泄漏事件依旧频传，一般民众对于自身权益保护的意识也日益高涨，且根据《个人资料保护法》第十二条的规定，若企业因违反该法而导致个人资料被侵害，“应查明后以适当方式通知当事人”。然而，第二十九条提及的企业损害赔偿责任，如果能“证明其无故意或过失者，不在此限”。因此，调查事件真相不仅仅是企业的义务，更是帮助企业保护自身的必要诉讼防守策略。计算机取证与调查势必成为企业应变个人资料泄漏事件的必要一环，本文将介绍企业进行个人资料泄漏事件调查时，在前、中、后三阶段可能面临的状况。

一、调查前置准备时

在事件调查行动开始前，专业的计算机取证调查顾问团队必须从环境架构复杂的客户端快速掌握信息且取得资源，才能确保后续调查过程的正确性与时效性。很多时候，由于人员的应变意识不足，或并不具备妥善的环境，又或公司内部并未取得共识，而直接造成对调查的阻碍或误解。因此，在企业与外部顾问共同展开调查时，企业应做好下述信息与资源的准备。

首先是事件背景资料的搜集，厘清究竟是哪些异常状况发生，导致企业认为有个人资料泄漏事件，包括异常状况发生在什么时间、发生于哪些主机或系统，并进一步记录该受害主机的平台环境，该主机开放的相关服务与事件发生时的网络联机状况，以及最重要的，事件通报或发现人员曾经执行过的任何应变动作。

其次是影响范围的初判，个人资料泄漏的起因通常不会只涉及单台主机，无论是外来因素或是内部因素造成的，牵连主机都可能包含数据库、相互间接系统平台、其他数据抛转主机，甚至是相同或互通网段服务器与用户主机等。唯有先取得前述系统/网络环境架构信息，并确认是否有类似或其他异常状况(仍在)发生，才能辅助判断事件的规模及程度，并开辟事件的“防火墙”。

在调查的初步范围确定后，应针对企业内部的科技环境现状进行确认，尤其是各种系统稽核日志，如同目前《个人资料保护法》实施细则修正草案第十二条第二项所要求的，“使用记录、轨迹数据及证据保存”，调查相关范围内的主机与系统，看它们是否皆具备稽核功能且妥善保存了足以帮助调查的轨迹资料。此外，

还要看企业是否具备并保存了联机防护设备监控的信息与异动记录。若企业已具备周全的证据保存环境，且曾经对于组织内的个人资料进行过盘查与流向清查，那么这些对于调查的进展都有极大的帮助。

前三项信息的取得可能都要依赖信息(系统与网络)安全部门的协助，但在计算机取证专业团队进行实地调查前，企业应建立起其他人员共同参与的共识，以便调查过程顺利进行。例如，管理高层的授权与布置，可以在外部顾问进行调查时，确保内部员工的配合度；遵法与行政方面的支持，必要时可包含法务、稽核、人资甚至总务与保全方面的协助。

二、事件调查启动时

在计算机取证专业团队进驻并启动调查后，若外泄事件持续发生，企业通常以应变防堵为优先作法，可能的系统下线、网络隔离、主机关机 etc. 都必须有专业人员进行实时取证与完整稽核轨迹留存作为相应的补偿措施，才不会导致事件调查的证据来源完整性受到影响。企业方面可能会有疑问是，科技环境架构如此庞大复杂，要从哪些主机着手才能查明事件发生的原因呢？以下介绍两种常见的实务调查方向。

(一) 由内而外进行调查

这种调查方式常见于个人资料泄漏事件已经明确发生，企业得知事件是来自外部机构通报或接到客户投诉等，但却不知外泄缘由。因此调查起点先定位于数据所在系统或主机，包括应用系统及数据库等；进而层层推进，向该主机有所间接、抛转、连接、互通的其他层面主机扩大调查。



(二) 由外而内进行调查

此种调查常见于已有外因造成的明显异常现象发生，由企业内部人员发现而主动通报，但尚无法确认哪些数据受害。因此调查起点先定位于外来联机的异常记录，如防火墙或IPS记录等；进而向内深入调查所有被接触过的主机及其延伸范围。

除了针对前面所提及的各种层面的完整稽核轨迹日志（包含数据库、网络防护监控设备、应用系统、服务器平台、操作系统、联机软件与防病毒软件等），进行人、事、时、地、物交叉比对的反常分析，以试图找出完整的犯规轨迹之外；针对单一嫌疑主机的深入调查也是十分必要的，专业人员利用特殊分析手法，在完全遵循数字鉴别原则的情况下，针对嫌疑者的行为执行数字取证。

三、调查完成后

在查明事件起因后，计算机取证专业团队会出具调查报告给管理阶层参阅，并对资讯人员提出相关强化方向的建议，将因事件所获得的数据文件完整移交给企业方人员；但若企业有委托保存数字证物的需求，则由外部专业数字鉴别实验室进行最严谨的数字证物托管，直到诉讼程序或委托结束。此外，假使企业认为有必要进行后续诉讼程序，鉴别顾问也会协助证据的呈交准备，并陪同企业代表（如法务人员）向执法单位进行证物的相关说明。

随着《个人资料保护法》逐渐为大众所熟悉，个人资料泄漏已成为企业不可忽视的潜在风险，对于事件查明的责任，已成为企业必须深思的议题。事件调查之前的企业准备、事件调查过程的实际方式与调查结束后企业所能获得的益处与后续帮助，皆可作为企业因考虑组织人力与公正性，而决定采用与专业第三方协同调查时，可遵循的良好实务经验。

企业敏感信息保护之道

肖青 经理

施建俊 副总监

德勤上海事务所
企业风险管理服务

回顾过去几年，因企业敏感信息泄漏而引发信息安全事件的有关报道不断见诸各种媒体，由此引发的种种风波，对相关企业的声誉、财务和合规方面都产生了不容忽视的影响。作为企业风险管理方面的专业咨询机构，德勤在与各行业的交流中，注意到企业决策层日益重视敏感信息防护，部分企业已经采用了数据泄漏防护（Data Leakage Prevention, DLP）等安全技术方案。这些产品在一定程度上为敏感信息建立了一道技术防线。然而，很多客户抱怨高昂的信息技术开支并没有明显改善企业在敏感信息保护方面的成效，一些用户由于日常工作受到功能复杂的安全工具的干扰，导致工作效率降低而不得不最终放弃之前投入巨资的保护方案。怎样才能全面有效地保护敏感信息，为企业经营管理保驾护航？我们听到了来自企业越来越多的疑问和困惑。

本文首先概述保护敏感信息的必要性以及DLP产品的主要功能及其局限性，然后介绍德勤在保护企业敏感信息方面的整体方法和思路，并探讨敏感信息保护体系为企业带来的价值。

一、何为企业敏感信息

近年来，企业的业务运转越来越依赖信息系统的支撑。企业中的大量数据，在不同业务部门、业务流程和信息系统间持续地生成、保存和传输，有时还需要与外部第三方进行数据交换。

一般而言，企业对于具有一定商业价值的信息都应采取必要的保护措施。其中具有重大商业价值，并直接影响企业竞争力和正常运营的核心数据一旦泄密，会给企业带来较大的声誉和经济损失，甚至面临法律风险或产生其他负面影响。这些核心数据，必须对其采取完整和充分的保护措施。这些也就是我们所称的企业敏感信息。

从存在形式来看，敏感信息可以是数据库信息、XML文件、应用系统内的数据、有详细属性的文件等结构化数据，也可以是邮件、模板、音频、视频、图像以及纸面文档等非结构化数据。从数据类型来看，敏感信息可以是经营管理类或技术类信息，也可能是员工或客户的隐私信息。数据所面临的威胁既可能来自内部，例如心怀不满的员工、合作伙伴等；也可能来自外部，例如商业间谍、网络钓鱼、黑客攻击等。

二、敏感信息保护正越来越受到企业重视

尽管大部分企业在战略角度对敏感信息保护的重要性都有一定认识，伴随着组织架构、业务范围、信息技术等不断变化，企业又常常顾此失彼。当前，敏感信息所处的外在环境愈来愈趋于复杂，敏感信息防护需求正成为企业决策者在信息安全领域最为关心的要素。

- 全球化。在世界不同国家和地区开展业务的企业，可能有不同的基础架构和信息管理系统，使用不同的第三方服务提供商，使用不同的采购和销售流程，面临不同的法律监管要求。

数据泄漏在不同行业和规模的企业中层出不穷。

- 数据流动。如果没有对敏感信息的流向和载体进行必要的控制，则敏感信息的跨部门、跨机构传播和复制存在很高的泄漏风险。
- 数据爆炸。据IDC统计，仅2010年，全球企业就产生和复制了过万亿GB的各类企业数据，超过之前5年内数据之和的9倍。规模的不断增长使企业敏感信息的有效管理成为更加复杂的挑战。

无论何种形式或类型的企业数据都可能面临来自内外部的威胁和攻击。

表1 常见的数据泄漏场景

使用中的数据 (Data in use)	<ul style="list-style-type: none">• 心怀不满或被解雇的员工将包含个人信息或机密信息的文件复制到移动设备上（例如U盘）；• 使用者在他人可以接触到的公众区域的设备上打印敏感信息
移动中的数据 (Data in motion)	<ul style="list-style-type: none">• 使用者为了在家工作，将敏感信息发送至个人邮箱或个人移动设备；• 为了商业目的通过不安全的传输协议与第三方共享个人信息和机密信息
存储中的数据 (Data at rest)	<ul style="list-style-type: none">• 商务人士不知情地将敏感信息储存在不安全的存储位置，不受企业IT部门的管理，如不可靠的第三方云存储平台；• 数据库的管理员将敏感信息的备份文件存储在未经批准的地方

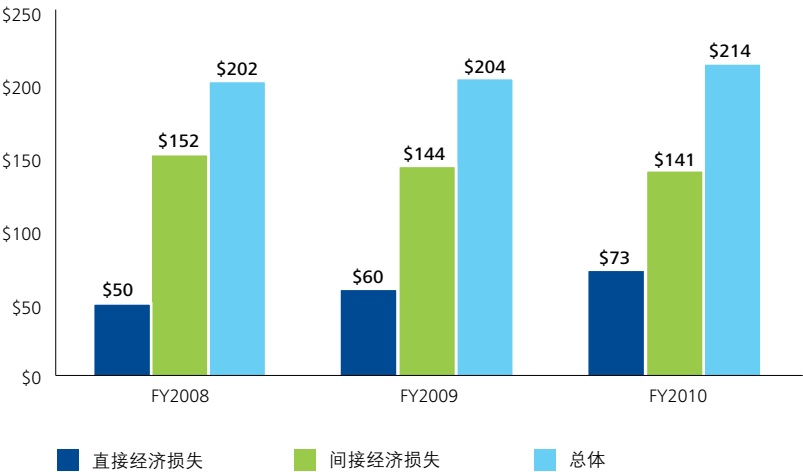


图1 数据泄露成本

资料来源：2010 Annual Study: U.S. Cost of Data Breach, Ponemon Institute, LLC.

- 移动技术和云技术的广泛运用。近几年，云技术和移动应用的迅速发展，如无线网络、移动存储、移动计算（例如iPad、智能手机）、云服务（IaaS、PaaS、SaaS）等，使信息的访问途径和方式得到了前所未有的扩展。据有关调查，约56%的公司认可并允许雇员在工作中使用个人信息处理设备，31%的雇员拥有的移动设备连接于公司网络，其中66%为笔记本，25%为智能手机，9%为平板电脑。

无论是有意还是无意，随时可能发生敏感信息泄漏（见表1）。

随着数据规模的不断扩大，越来越多的数据泄漏事件随之而来。近年来的趋势表明，企业敏感信息已经渐渐成为企业不正当竞争甚至网络犯罪的牺牲品。在利益的驱动下，一些敏感信息可能最终被泄露给竞争对手或是不法分子。近些年各行各业信息安全事件证明了这一点：

- 2012年3月：某保险公司泄漏了上千投保人和受益人的电邮地址。
- 2011年10月：某零售企业泄漏了包含大量机密客户信息的EXCEL文件。
- 2011年7月：某保险企业泄漏了700多条个人姓名和社保账号信息等客户机密信息。
- 2011年4月：某信用卡加工公司，在重大的数据泄露事件中泄露了众多邮件地址。

进一步的研究还表明，在处理敏感信息泄漏的过程中，事件监测、事件通报、事件响应、长远业务损失等每个环节都会带来额外的成本和其他负面影响，图1列示了Ponemon Institute对数据泄露成本的调查。

最近Gartner的一份调研报告显示，相当比例的高层受访者表示，他们将数据保护列为企业最优先考虑实施的安全技术之一（见图2）。

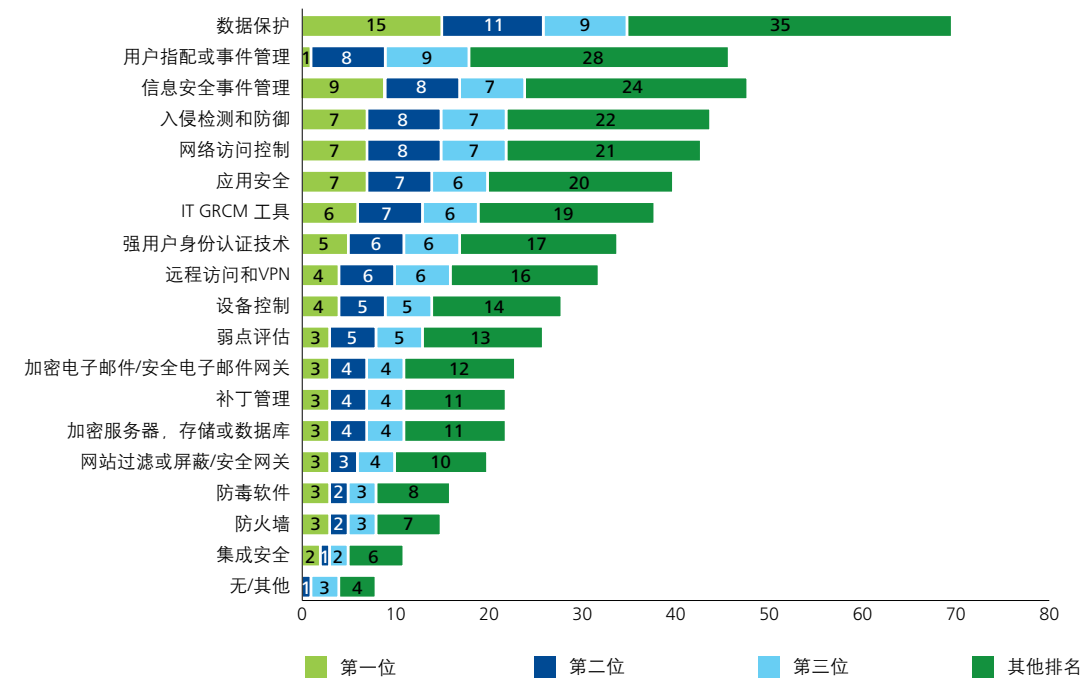


图2 企业考虑实施的安全技术排名

资料来源：Gartner — User Survey Analysis: 2012 Security Buying Behaviors and Budget Trends, November 2011.

三、数据泄漏防护工具的局限性

越来越多的企业开始考虑运用DLP工具来保护企业的敏感信息。DLP工具的主要作用是对敏感信息流入、流出企业及在企业内部的流转存储和终端操作等进行技术管控，如进行实时监测、警告和阻断等，也可进行离线的深度分析（见图3）。



图3 DLP工具的功能模块

DLP工具可以部署在企业的存储、网络和终端设备上，例如：

- 存储。DLP工具的一个基本功能是能够找出特定的文件，例如电子表格和文字处理文档，不论它们保存在文件服务器上、区域网络上，或是在终端上。一旦找到之后，DLP工具还会对文件内容进行扫描来确定是否存在敏感信息。
- 网络。使用特定的网络技术对网络流量进行捕捉和分析，并能够检查传输中的数据。如果发现敏感信息的流向未经授权，DLP工具可以根据预先定义的规则发出警告并阻挡数据流。
- 终端。一般通过运行客户端Proxy软件来实现对本终端操作的管控。终端管理主要旨在管理用户在工作站上进行的数据移动操作，例如拷贝数据到U盘、发送信息到打印机、在应用程序间剪切和粘贴等。

但是，随着企业信息安全建设的深入，企业往往会发现，仅通过部署DLP工具并不能很好满足管理层对敏感信息保护的期望。主要面对的挑战和原因如表2所示。

因此，我们认为要建设持续有效的企业敏感信息保护体系，必须从整体的角度出发，不仅需要关注技术，更要关注治理、人员组织和流程，建立自上而下的保护体系。

表2 DLP工具面对的主要挑战及原因

挑战	原因
DLP工具不能完全满足企业的管理需要	• 缺少适当的信息安全战略和敏感信息保护策略
难以评价DLP工具的业务价值	• 没有明确的度量指标和评价标准； • 难以收集和报告度量指标
文档加密的密钥管理困难	• 理解误区：加密作为技术措施，难以满足管理控制的需要，常常对不同密级的数据施行了单一的加密策略
人员的信息安全意识没有因此提高	• 很少或没有明确的培训、意识和沟通计划
DLP未与其他安全事件及其相关风险关联	• 缺少与信息安全与事件管理(SIEM)的整合； • 缺少与风险管理和合规管控的整合
被过多的信息安全事件“淹没”	• 没有明确定义信息安全组织的角色和责任； • 没有明确的信息安全事故的处理机制； • 缺少从大量安全事件中过滤出高风险事件的机制
未分类的敏感信息	• 很少或没有明确数据的分类分级管理制度； • 用户的安全意识不够； • 未施行更自动化和智能化的技术

四、企业敏感信息保护体系

企业敏感信息保护体系应该与企业信息安全保护体系紧密结合，在治理、人员、流程和信息技术各个层面综合考虑。

(一) 治理

敏感信息安全战略应当与企业信息安全规划紧密结合，并考虑企业战略、IT规划、风险管理和合规要求等，并在制订和推行过程中争取企业高层的充分支持和参与。企业应当认识到，加强敏感信息保护和信息安全的工作并不是一次性地对信息技术做出投入，而是一个建立并持续改进的过程。总体而言，企业敏感信息规划中应当包括下列专题：

- (1) 信息安全和敏感信息保护策略；
- (2) 信息安全治理的组织架构；
- (3) 安全与系统开发和采购的结合；
- (4) 信息分类的级别定义；
- (5) 风险管理战略；
- (6) 应急计划和事故处理；
- (7) 信息安全意识和培训；
- (8) 法律和规章责任；
- (9) 外包管理。

(二) 人员

信息安全不仅仅和IT人员有关，而是和各业务条线、各层级管理人员都有关系。建立适当的信息安全组织对企业范围内的敏感信息进行保护，并对职责进行合理分配和划分。具体来说，企业中需要下列信息安全角色：

- (1) 信息安全协调小组，负责协调跨部门/业务单元的信息安全问题；
- (2) 高层信息安全官员，负责处理企业内与信息安全相关的事务，并与管理层持续沟通。

信息安全协调小组和高层信息安全官员应具有明确规定的职责和足够的经验。企业应为高层信息安全官员提供明确的沟通路径、角色和充分的授权，并由信息安全协调小组审批。

此外，企业还应当考虑为关键项目和应用系统指派信息安全专员，并向高层信息安全官员负责。这些专员的职责包括制订和实施专门的安全计划，对信息安全防护措施的实施和使用进行日常监督，以及协助调查信息安全事故等。

(三) 流程

为了有效地保护敏感信息，可结合企业的信息安全管理现状，有针对性地制订一系列管理制度和标准，包括：

- 信息安全流程制度，包括信息安全方针、信息安全组织、资产管理、人力资源安全、物理和环境安全、通信和操作管理、访问控制、信息系统获取、开发和维护、信息安全事件管理、业务连续性管理、符合性等方面。
- 敏感信息安全管理流程，包括通信传输管理、存储管理、移动介质管理、归档管理、超级用户管理、第三方信息交换管理、日常操作管理等方面。
- 信息分类分级管理流程和制度，包括数据资产密级划分、数据资产分类管理等方面。
- 信息安全内部审计管理，包括信息安全内部审计框架、信息安全管理有效性衡量指标等方面。

建设企业敏感信息保护框架，不仅需要关注技术，更要关注支持和配合系统的人员组织和流程。

(四) 信息技术

针对承载敏感信息的信息技术环境所存在的弱点和威胁，提出相应的技术风险处置建议。根据企业的风险接受程度和优先级，技术措施可以包括以下内容：

1.改进现有系统的信息安全控制

通过配置改进等系统优化方法，增强网络设备、服务器、软件、终端、存储等薄弱控制环节。相对而言，这类针对单一控制点的改进措施的投入成本较低，可在短期内改进完毕。

2. DLP产品

根据企业自身需求和数据保护的技术措施建议，选择实施主流的DLP产品，从终端、网络和存储方面，对特定的高风险领域实施技术管控措施（见表3）。

表3 主要的技术管控措施

挑战	根本原因
终端控制	<ul style="list-style-type: none">• 根据保护策略，监视用户的数据交互以识别未经授权的操作，例如，企图转移敏感性的内容到移动存储设备；• 禁止未授权的复制、打印、截屏、打开、粘贴、另存为等操作
网络控制	<ul style="list-style-type: none">• 根据保护策略，分析网络中的数据通信以识别敏感内容通过e-mail, IM, HTTP或FTP，实施准入、审计、隔离、限制、加密和通知等控制措施；• 整合邮件传输代理、网络组件和其他基础设施
存储控制	<ul style="list-style-type: none">• 根据保护策略，扫描和检测企业数据储存库以识别敏感内容，并相应地实政策略

3.身份管理和访问管理

通过单点登录，联合身份认证等技术，IAM可以帮助统一不同应用系统间的用户身份，有效施行访问控制矩阵和职责冲突检查，为更自动化和智能化的敏感信息保护体系做好准备。

4.安全事件响应和事故管理

SIEM产品通过连接企业的不同系统并对海量信息安全日志进行实时分析和监控，自动化和智能化地识别出需要及时响应的安全事件，保证高优先级的安全事件能够得到及时响应和处理。

五、德勤的敏感信息保护方法论

德勤的敏感信息保护方法论已经协助不同行业和规模的企业建立了行之有效的保护体系。总体来看，我们的方法是首先协助企业建立企业敏感信息保护的管理体系，再根据企业自身需求提供恰当的技术实施方案。

在体系建设中，德勤协助企业规划和建立以敏感信息保护为重点，兼顾企业信息安全管理需求的信息安全管理体系。体系建设的主要工作有：信息安全成熟度和差异分析、敏感信息分析、风险评估及风险处置、敏感信息保护建设规划。在安全产品的技术实施方面，德勤为企业进一步提供产品选型、质量保证或产品实施服务。

需要指出的是，我们的整体方法可以基于企业需求和保护目标来定制（见图4）。

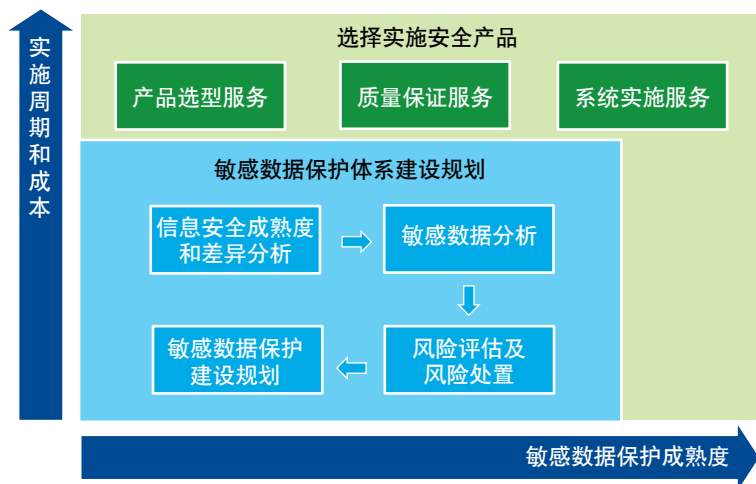


图4 敏感信息保护体系建设整体方法和主要步骤

（一）敏感信息保护体系建设

不难看出，体系建设是企业敏感信息保护体系的核心工作，也是实施产品的前提。以下将展开介绍这部分工作，并以敏感信息分析和风险评估为例介绍分析方法。

在体系建设中，我们的工作将分为以下几个步骤：

- (1) 从客户自身需求和法律法规、行业监管要求、合同协议等方面切入，以德勤信息安全管理框架为基础，经过信息安全成熟度分析和差异分析，了解企业的信息安全现状；
- (2) 调研敏感信息的分布情况、存在形式、业务类型及业务影响；
- (3) 进行数据分析，识别数据经过的组织和人员以及承载数据的各类信息载体等要素，进行风险评估，并制订相应的风险处置计划；
- (4) 最终根据所指定的风险处置计划，自上而下地建立以敏感信息保护为重点的信息安全管理体系。

（二）人员参与

在敏感信息保护体系建设的过程中，适时和充分的人员参与至关重要。企业或组织应该建立信息安全委员会指导该项目的活动，并在授权范围内充分调配企业的各项资源给予支持。

在制订正确的保护策略、识别业务数据生命周期、明确数据责任人、进行风险评估等工作中，都需要管理层和不同业务条线的参与和判断。从我们的经验来看，下列人员应该参与：

- 法务、隐私、公司安全、信息安全人员。
- IT工程和运营人员。
- 人力资源管理和员工代表。
- 关键业务代表。
- 高级管理层。

还应当制订信息安全意识和风险管理等方面的培训计划以保证员工能意识到自己的工作角色和职责，确保需要接触敏感信息的员工接受了和公司安全策略相一致的适当培训，并且保证只有有业务需求的员工才能接触到敏感信息。

(三) 敏感信息分析和风险评估

风险评估通过对敏感信息相关的信息资产进行调研分析，识别出与之相关的弱点和威胁领域，进而评估敏感信息所面临的风险。所以在体系建设工作中，风险评估起着关键作用，直接影响到后续的风险处置计划。

敏感信息经过的组织、人员和系统等信息载体，既是风险评估过程中必不可少的输入项，也是评估敏感信息泄露风险的基础。因此准确和完整地识别各类敏感信息的信息载体，是体系建设的重中之重。

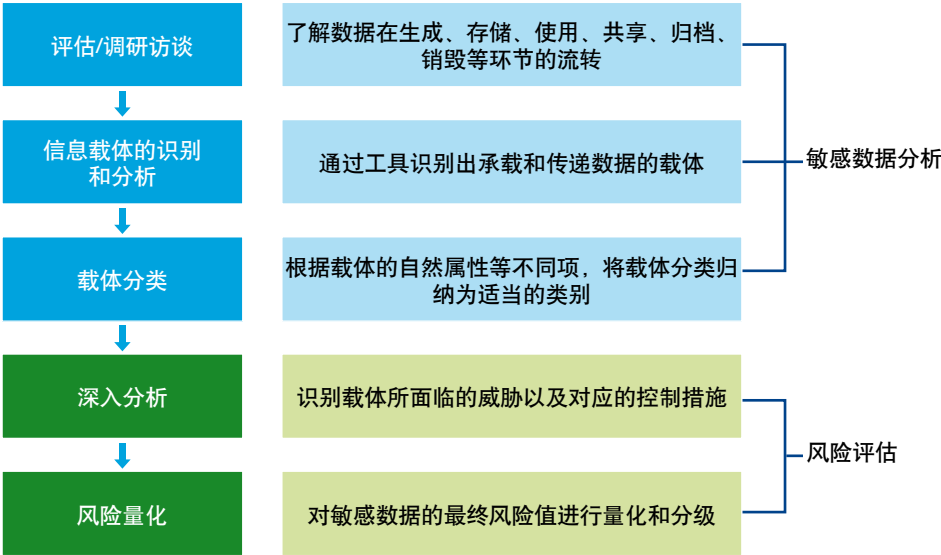


图5 敏感信息分析步骤

1.调研访谈

通过对敏感信息相关责任人和其他负责人的访谈，了解数据的业务实质，以及数据在生成、存储、使用、共享、归档、销毁等不同环节的流转过程。

2.信息载体的识别和分析

根据所了解的情况，通过工具分析，识别出人员、软件（系统）、硬件（系统）、服务（内部/第三方）等承载和传递数据的载体。

表4 在载体识别分析过程中每个环节须考虑的输入项

敏感信息	生命周期环节	数据形式	数据类型	泄漏影响	数据载体	保密期限	责任人
敏感信息的定义	可以是生成、存储、使用、共享、归档、销毁等环节	可以是电子数据或纸面数据	可以根据数据的业务实质、数据的流转途径确定数据类型	敏感信息一旦泄漏可能造成的影响，应综合考虑财务和非财务影响，例如商誉、法律风险等方面	视具体情况而定，可以有硬件、软件、人员或者内部/第三方提供的服务等	敏感信息的保密期限	经管理层认可，负责信息的生成、开发、维护、使用和安全管理的人员

3.载体分类和整合

依照载体的自然属性、所面临的特定弱点和威胁等，将载体分类归纳为风险评估的输入项。

4.深入分析

结合现有的风险控制现状和风险管理办法，识别载体所面临的威胁以及相应的控制措施（见表5）。

表5 不同的威胁环境描述

威胁种类	威胁描述
通信传输	防止敏感或机密数据可能通过邮件、即时通讯软件或网站应用程序在组织内外部分发或扩散
数据/文档/集中存储	未经授权地访问存放在企业数据库/个人电脑/档案室里的数据，包括数据库、邮件服务器、文件服务器、个人电脑和档案室等
移动介质	移动介质的丢失或者未经授权的访问，包括笔记本电脑、PDA、手机、U盘、光盘和纸张等
归档及保存	未归档或处置的数据及载体，由于保护不当而造成的损失，包括纸张、磁记录介质等
拥有特殊权限的人员	拥有特殊权限的人员导出和复制数据所造成的敏感信息泄漏
第三方信息交换	提供与外包、联合开发、市场营销和供应商之间的关系合同的敏感信息保护，涉及跨组织、地理和系统边界的数据传输安全
日常业务处理	敏感信息在日常的业务处理过程中流转时，被恶意的人员窃取

5.风险量化

对敏感信息的最终风险值进行量化和分级。具体来说，是综合在生命周期中各环节承载敏感信息的载体的风险控制措施、弱点暴露程度以及风险损害程度，并结合敏感信息的影响程度，计算出风险终值。



六、敏感信息保护体系的价值

敏感信息保护体系对于企业组织的战略、运营和管理等方面具有重要的意义：

保护关键业务数据和知识产权。敏感信息保护体系的主要价值之一是更好地保护关键信息免受泄漏。企业中保存了许多类型的信息，出于竞争、合规要求、声誉影响等理由需要对它们进行保护。

减少数据破坏的风险。通常数据泄漏事件会对企业造成一定的财务影响，通过减少数据泄漏的风险，可以降低企业的财务风险。

增强管理层信心。完整的敏感信息保护包括了战略和规划、组织和人员、员工培训和意识教育程序、管理流程和数据保护制度，以及相应的技术措施等内容。它使管理层确信，企业范围内的敏感信息已经在组织各层级得到了充分重视，进行了充分的识别和分类，依据不同的风险，区分施行了必要的保护措施。

消除合规风险。根据相应的法律法规和合同/协议等要求建立的敏感信息保护体系，将消除因数据泄漏或审计发现等而导致处罚的风险。

七、结束语

众多企业已经认识到敏感信息对于企业的生存和发展至关重要，是企业最值得保护的信息资产。一旦发生意想不到的数据泄漏，所引起的经济成本、隐性成本及法律风险，可能使企业面临不堪承受之重。

为了提高企业管理关键数据资产风险的能力，全面的敏感信息保护应自上而下，由战略和人员意识、组织架构和职责、流程制度和技术措施等部分组成。充分的计划和准备、必要的沟通、贯穿始终的安全意识教育等都是保障项目成功的重要因素。

银行信息科技安全风险管理的探讨

何 微 副总监

德勤深圳事务所
企业风险管理服务

中国银监会于近期发布了《银行业金融机构信息科技外包风险管理指引》，这是银监会自2009年发布了《商业银行信息科技风险管理指引》后，根据信息科技的发展形势，在信息科技安全风险方面适时出台的系列信息安全风险管理政策、办法和规定之一。另外，银监会在2012年成立了信息科技监管部，种种迹象表明，信息科技风险管理将成为日后信息科技监管的重点。

随着经济的快速发展和对外开放的不断深入，我国银行业务快速发展，同时信息科技也呈专业化、集中化、规模化的发展趋势。信息科技与业务的联系越来越紧密，不仅成为业务开展的必要基础支持，甚至于在部分传统业务领域，信息科技已开始引导银行由传统业务向信息科技变革。

随着监管机构的合规要求越发全面与严格、银行内部对于信息科技管理要求的不断提高、大数据的高度集中化、与第三方机构合作的内容与形式日趋多样化，信息科技安全的风险隐患也日趋严峻。信息安全风险将远远超出操作风险的定义，如何做好信息科技安全风险管理工作，将成为银行抵御互联网金融对传统金融行业的冲击，提高核心竞争力的工作重心之一。因此，建立与信息科技发展趋势相适应的信息科技安全风险管理体系，已成为当前银行信息科技风险管理工作必须关注的重点。

一、现状

当前银行业大多将信息科技风险作为操作风险的一部分，纳入银行全面风险管理体系当中进行统一管控。但是，信息安全风险具有其自身的特殊性。

- (1) 范围延展性。按人们传统思维的理解，信息科技安全的范围仅仅指电脑系统里的符号组合，如数字、文字、图像，或是计算机代码等虚拟数据。但随着信息技术的发展，信息载体的推陈出新，信息科技安全的范围定义不断被放大，除了电子化的数据外，还包括了各种非电子化的信息载体（如书面文档、U盘、备份磁带，甚至员工手机等自携设备等）。

- (2) 复杂与不稳定性。随着银行核心业务系统不断的功能开发，银行各业务条线的业务操作越发依赖于系统平台；业务外包的内容不断增长，形式越发复杂；日新月异的信息科技发展对传统银行业务的冲击越来越大。由于管理因素、技术因素的多重作用，导致偶发性和不确定性突出，使得风险控制的复杂度大幅提高。

- (3) 成本损失不确定性。信息系统一般支持多个业务，如发生事故，所造成的直接成本损失非常小，但造成的间接损失影响范围往往涉及面广且难以评估其影响与损失。如某分行柜台系统后台服务器由于信息安全事故而不能正常运作，其直接损失可能仅为一台服务器主机的成本，但所带来的间接损失的影响面却非常广，如额外维修所产生的人工和硬件成本、受其影响而无法操作柜台业务所带来的业务收入减少、由于银行不能持续为用户提供柜台服务所带来的声誉损失等，这部分的损失涉及因素众多而且非常难以计算其损失金额以及恢复成本。

因此，随着银行业务的发展和技术进步，在操作风险模式下管理信息科技风险也存在明显的困难。一是目前的操作风险管理方法中对信息安全风险的管理方法涉及较少，难以兼顾信息安全风险的技术专业性，难以实现对信息安全风险的有效管理；二是风险监管资本计量未能充分考虑信息科技风险因素，信息安全风险造成的损失及其相应的监管资本计量存在一定的困难。

基于信息科技安全风险的自身特点及其管理中遇到的特有挑战，应对信息科技安全风险进行独立管理。

二、思路

针对银行信息科技风险管理的特点，我们设计了银行信息科技安全风险管理体系（见图1），为银行提供全面、灵活、高效的信息科技风险管理整合解决方案。



图1 银行信息科技风险管理体系

方案以德勤“信息安全风险管理框架”为基础，设计灵活的接口以结合外部环境监管以及银行内部管理等多层次要求（见表1）；再配套统一的工作方法论、流程、标准，完善银行现有的信息科技风险的战略、计划与制度，搭建高效的沟通平台，形成银行量身定制的信息风险管理体系。该体系在完全融合银行现有体系的基础上，提供了开放性接口的管理工具，既能减少因体系变更所产生的变动成本，又能从容应对信息科技安全风险管理将来的各种变化与挑战。

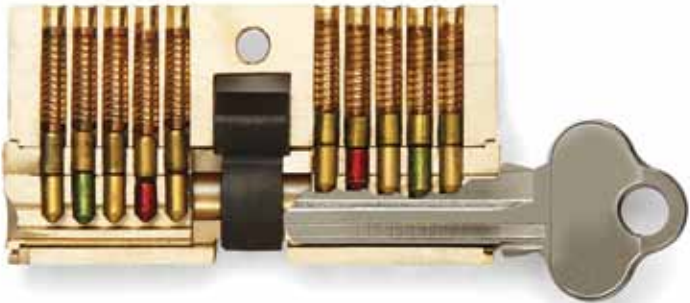
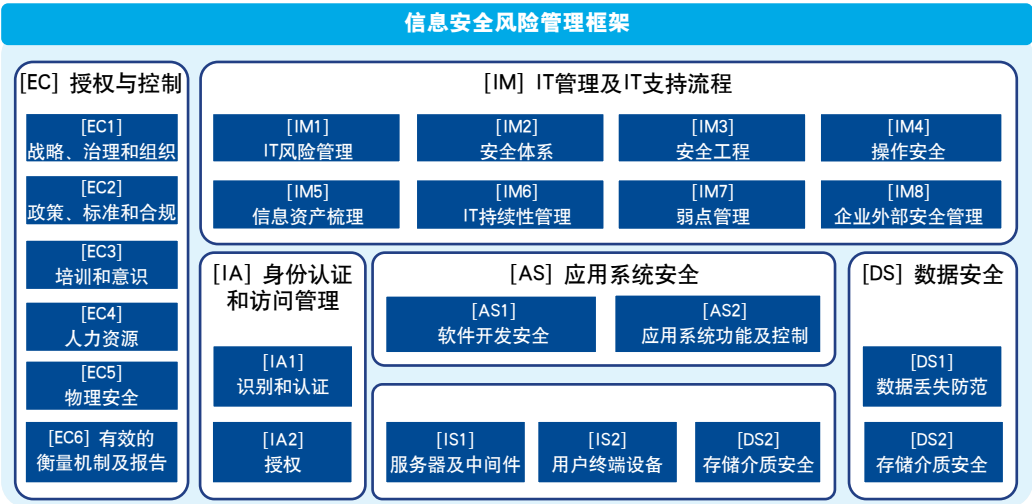
表1 银行内部、外部以及其他相关要求部分示例

	内容	提出单位
内部管理要求	银行内部审计要求	内部审计部门
	操作风险管理要求	操作风险管理部门
	IT部门内部操作规范要求	IT运维部门
	总行信息科技相关制度要求	IT内控部门
	各分/支行信息科技管理制度要求	分行IT部门
外部监管要求	银监会相关监管要求	银监会
	外部审计要求	外部审计单位（会计师事务所）
	央行相关信息科技管理制度要求	人民银行
	中国——《企业内部控制基本规范》（C-SOX）	财政部、各证券交易所、内控委员会等
	中国香港——《第21项应用指引》（PN21）	
其他相关要求	美国——《萨班斯-奥克斯利法案》（US-SOX）	
	国标——信息系统安全等级保护（GB/T 28448-2012）	国家标准化管理委员会、信息安全标准化技术委员会
	国标——信息安全管理体系要求（GB/T 22080-2008）	
	国标——个人信息保护指南（GB/Z 28828-2012）	
	ISO 27001 / ISO 20000 / BS 10012 / ISO 22301	ISO / BSI
	移动支付安全标准	人民银行 / PCI
	外包服务合同要求	外包管理部门 / 外包需求部门

德勤的“信息安全风险管理框架”结合了国内外的行业标准以及最佳实践（如COBIT、ISO 27001等），从授权与控制、IT管理及IT支持流程、身份认证和访问管理、应用系统安全、架构安全、数据安全六方面阐述了企业信息资产在完整性、可用性及保密性等方面面临的信息安全风险以及相应的内部控制目标。该框架提供了信息安全风险的评估测试指导并可作为预设的成熟度模型，从战略的层面支持改进企业的信息安全管理。

三、实施

第一阶段，我们以德勤的“信息安全风险管理框架”为基础，同时与银行外部监管要求以及其他相关要求等不同方面的要求进行匹配，基于上述要求补充并完善“信息安全风险管理框架”里的风险及对应的控制措施，生成银行信息科技安全风险控制基础库（见图2）。



第二阶段，我们以银行信息科技安全风险控制基础库为基础，针对银行需求挑选外部要求与标准、银行内部的内审要求以及相关的制度法规，识别银行独有的风险以及各控制措施，为银行定制适合其需求的信息科技安全风险控制库。并以此控制库为核心，完善相关的工作规划、流程、底稿模板、风险评估标准等，从而逐步完善其信息科技风险管理体系。

四、应用与价值

(一) 统一规划，改善沟通，提高效率

以信息科技安全风险控制库为基础，综合统一管理内/外部的多层次要求，形成统一的检查工作流程和模板，并以此为基础开展信息科技安全风险审计工作。

加强“总行—分行—支行”在信息科技安全管理中的协同性和一致性，有效管理信息传达的一致性，减少在应对内部（如信息科技部门与业务部门）以及外部（如监管机构的监管要求）的不同需求时的反复沟通，避免沟通信息失真，从而提高信息科技安全风险管理的效率。

使用统一标准的测试流程以及工作模板，基于“总行—分行—支行”统一高效的沟通与理解，减少应对各层面的繁复检查工作，高效执行信息科技安全风险测试评估工作，提高工作效率。

(二) 完善现有信息科技风险管理体系，优化资源规划

在体系的建立过程中，可同时梳理现行制度。利用信息科技安全风险控制库，将监管要求与银行内部制度做横向对比，即可发现银行现行制度与相关的监管要求之间的匹配情况，从而清晰定位出现行制度的“空白区域”，为完善制度体系提供全局视图。

通过不断汇总收集各种信息科技检查工作的结果反馈，包括总行各业务条线的相关IT支持，汇总并分析测试结果，结合固有风险评估结果，对剩余风险执行多维度的综合分析（如不同风险领域、不同级别类型的分行等）。根据分析结果更合理地对有限的IT资源进行规划，优化检查工作计划并调整各分行的检查重点，以提高每次检查工作的针对性、有效性，为信息科技安全风险管控规划提供基础。

(三) 及时更新以应对内外环境的不断变化

信息科技安全风险管理体系应迎合内外部环境的变化而不断更新，以使银行能及时响应信息科技安全风险变化的需求。可从两个方面进行体系更新：

首先，银行要根据业务战略目标调整、信息安全管理水平提升、内部制度以及信息安全工作规范变更等内部影响因素，自行持续更新信息科技安全风险管理体系中的风险控制活动内容。

同时，我们也将充分利用丰富的金融行业咨询业务以及相关的金融企业审计经验，及时洞悉监管要求以及行业标准等外部环境的变化动向，向银行不定期发布更新包，保证其信息科技安全风险管理体系的及时性与完整性。

五、结束语

随着信息技术的飞速发展，银行业对信息科技的依赖越来越大，大数据、云计算、物联网等新技术既加快了银行业的创新发展，也对信息安全风险管理提出了更高的要求。快速变化的外部环境，开放的互联网环境，技术类企业、第三方平台等非金融机构与银行业的业务服务不断融合等，所有这些都使得信息科技安全风险管理与监管面临着更加现实的挑战，需要我们不断地思考和研究，提高信息科技安全风险管理能力，以适应内部发展要求以及外部不断变化的环境。

当前宏观背景下租赁行业的机遇、风险和创新



俞开琪

上海锦祺金融顾问有限公司董事长

全国人大《融资租赁法》立法顾问

原上海市租赁行业协会会长

2012年，我国面临着严峻而复杂的国际国内经济形势，发达经济体增长乏力，国际金融危机的深层次影响仍在持续，世界经济的不稳定性、不确定性上升，而我国经济在增长模式上仍存在严重的体制性矛盾和结构性问题，面临迫在眉睫的经济转型。此时，融资租赁业应运而生，同时具备金融、贸易属性的可持续发展的新型服务业迅速崛起，以融资、理财、促销的强大功能展现其独特的魅力。然而，如何适应中国经济转型的要求，如何应对融资租赁业面临的极大的行业风险，融资租赁业亟需创新和解决深层次的问题。

一、中国经济转型迫在眉睫

世界经济发展迄今，粗放型的增长模式已宣告终结。从技术经济学和新制度经济学的基本理论来看，建立在技术研发和制度安排基础上的经济增长才是最具竞争力的增长模式。如果这个基本判断是正确的话，那么，当我们回过头来看中国经济增长模式，中国经济转型迫在眉睫！

- (1) 高速增长以房地产为龙头的产业模式已不可维系，让房地产回归理性轨道，而不是任其一味地绑架中国整体经济运行，已成为当前最为重要的抉择。
- (2) 着力消除国有企业和民营企业之间的巨大不平等，营造健康的经济结构。中小企业的发展是一个国家经济发展健康程度的重要指针。
- (3) 资源消耗型经济结构应予以终结，建立在强大的技术研发和自主创新基础上的新型经济发展格局理应成为我国未来经济发展的真正引擎。
- (4) 产品外销模式应当转变为优化国内消费模式。建立在低人力成本优势基础上的中国低端产品制造业将面临越来越严峻的挑战。

由此可见，中国经济增长的不稳定因素不在市场而在于制度设计，如果不能有效消除增长模式上严重的体制性矛盾和结构性问题，不能有效消除流通环节对基本消费品的价格掠夺，未来中国通货膨胀和产能过剩的矛盾将会成为危害经济健康发展的罪魁祸首。

专家指出，中国经济将面临四大转型：

- (1) 从投资主导向消费主导转型；
- (2) 工业化主导向城市化主导转型；
- (3) 从私人产品供给向公共产品供给转型；
- (4) 低碳经济转型。

中国的宏观经济形势从侧重于保增长转到侧重于调结构，必须面对的一个现实就是要转变经济发展方式，即所谓的经济转型。促转型是长远之计，不仅仅是一年，而是连续几年，需要比较长的时间才能完成。社会制度转型，经济体制转轨，发展方式转变，这意味着中国又进入了一个新的历史阶段。

新的历史阶段和新的经济发展方式必须要赋予新的内容和使命，必须有新的、功能完善的、创新能力强大的服务产业相配套，而集金融属性与贸易属性于一身的、功能强大的现代服务业的代表性产业——融资租赁业将应运而生、迅速崛起。

二、中国融资租赁业正在迅速崛起

融资租赁是当今国际上发展最迅猛的现代新兴服务产业之一，也是世界上仅次于银行信贷的第二大金融工具，全球目前通过这一方式完成固定资产投资高达15%~30%，完成飞机、船舶、工程机械等大宗商品销售达50%以上。在许多发达国家，融资租赁总额占GDP的20%以上，融资租赁业是全球发达国家的“朝阳产业”。

在金融管制的中国，融资租赁是非银行金融机构经营金融业务的少有几个方式之一。由于长期以来相关部门监管过度，进入门槛较高，该行业一直发展迟缓。当前，由于银行控股的金融租赁公司和商务部系统内融资租赁公司试点放开，外商独资、中外合资的融资租赁公司审批权下放，国家有关部门对融资租赁的配套政策也逐步到位，极大地推进了金融市场业务多元化、综合化、专业化发展，也成为我国拉动内需、刺激消费，盘活存量资产，推进政府城市基础建设和“三农”建设的重要金融工具，2011年中央首次将融资租赁业务写入中央一号文件。

自2007年起，由于金融租赁的试点开放，中国融资租赁业一直呈几何基数增长，业务总量由2006年的约80亿元增至2011年的约9300亿元，共增长了100多倍；“十二五”期间，融资租赁业务将继续快速增长，2012年中国融资租赁总额达到约13000亿元。随着中国融资租赁业的迅速崛起，这一现代服务业在经济社会中的作用开始凸显。

尽管如此，目前中国融资租赁市场渗透率仅为3%，而世界融资租赁市场渗透率已接近17%，美国一直保持在30%左右，国内租赁业发展远未满足经济发展的实际需求。作为融资租赁行业的“四大支柱”，监管、法律、会计、税收政策环境尚有较大提升空间。中国在租赁融资、理财、促销的功能远未发挥出来，90%以上的融资租赁市场还处于空白。

三、融资租赁业将面临极大的发展机遇

融资租赁是中国经济发展到一定阶段的必然产物。融资租赁迅速崛起的根本原因是融资租赁的发展顺应了中国经济的发展，尤其是融资租赁业的融资、理财、促销三大主要功能恰恰能满足转型中的中国经济所迫切需求的市场化运作，是科学发展观在现代服务业产业属性中的具体体现，也是经济方式转变中最具可持续发展的、符合低碳经济的新型行业。

(一) 融资租赁在经济转型中的融资功能

融资租赁和银行贷款其实是异曲同工，都是为企业融资，只不过融资租赁是通过融物达到融资的目的。融资租赁最显著的特点就是能够在租赁期间将设备的所有权和使用权相分离，因此同样是融资，银行仅仅拿到了债权，而租赁公司却同时拥有了债权和物权，一旦承租企业破产，租赁物可以收回变现。因此，融资租赁行业不同于银行，它的抗风险能力特别强大。在中国经济转型中，它的作用非常显著。

- (1) **可以成为解决中小微企业融资难的生力军。**尤其和政府政策性担保及银行联动，可以大大降低中小微企业的融资门槛，增强政府担保以及银行对中小微企业的运作力度。
- (2) **可以服务实体经济。以设备和设施为租赁标的物的融资租赁业大大优于银行按揭等金融工具。**融资租赁以为客户购置设备为基础进行融资，有利于控制贷款方向，也有利于促进设备贸易的发展。

- (3) **可以成为解决西部资金缺乏的新通道。**通过开展对西部的融资租赁业务，既可以把东部的产品租销到西部，又解决了西部资金不足问题，起到“东资西调”的作用。

(二) 融资租赁在经济转型中的理财功能

融资租赁不仅是一种新型的融资方式，能够更好地帮助企业融资，而且能优化资源配置，提高各种经济资源的利用效率和发展质量。融资租赁在发达国家是一种高级理财工具。通过售后回租等方式，可以盘活企业的存量资产，加速现金流动；可以改善财务报表，调整财务结构；可以减少资产闲置，提高资产回报率。在中国经济转型中可以起到以下几方面作用：

- (1) 采用融资租赁可以提升国有大中型企业的效益和管理水平。提高资产回报率、资金周转率、资金流动性等企业的重要管理指标。改变企业单纯依靠廉价劳动力生存的低水平经营现状。
- (2) 推行融资租赁方式可以提升我国实体经济的轻资产管理能力，提高经济运行质量，提高企业的国际竞争力。
- (3) 通过融资租赁和经营性租赁可以推进新产品开发，促进产品的更新换代，加速科技型企业的发展。

(三) 融资租赁在经济转型中的促销功能

通过融资租赁促销是发达国家租赁业发展的主旋律，大到飞机、轮船，小到家具和办公用品都可以用类似按揭的融资租赁办法去租买。融资租赁是一种信用消费，今天用明天的钱；融资租赁是分期付款式的购买，使得各种不愿意一次性付款而善于理财的人们能够灵活地消费。因此，租赁行业在美国特别发达，通常占有全社会固定资产投资和社会消费的30%以上，而我国长期以来仅仅为1%左右，近几年虽然在迅速崛起，但是与全社会固定资产总额相比，还不足5%。所以说融资租赁市场空间特别巨大。

因此，大力发展融资租赁业，对转型过程中的中国经济在拉动国内消费上起到得天独厚的作用，是改变当前我国经济中一味地靠投资主导拉动和产品外销模式拉动而转为内需拉动的十分强大的工具。

- (1) 融资租赁有强大的激发潜在客户有效需求的功能,使一时没有购买能力的客户通过分期付款达到了购买目的。据国际和国内的市场调查,融资租赁可以激发85%的客户有效需求,特别能推动在国民经济中占大比重的飞机、船舶、大型的机电产品、装备类产品、能源、化工、基础设施等产品的促销。将在刺激内需、发展实体经济中发挥独特的巨大作用。
- (2) 通过所有权和使用权的分离,加上高科技的风险防范手段,使客户的购买门槛大大降低,如民营企业甚至私人客户都可以采取零首付的方法来租赁价格昂贵的工程机械设备,通过边施工、边还款的方法最终将设备买下来。有利于中小微企业的发展。
- (3) 利用融资租赁对外促销本国产品有很多好处:①租赁出口不同于普通货物对外贸易出口,能有效地规避进口国的各种关税的贸易保护主义的限制。②利用租赁出口可以有效地享受进口国的优惠政策且不违反WTO规则。③利用租赁出口可以不像出口信贷要接受各国国际惯例,特别是世界经合组织(OECD)的出口信贷“君子协定”的约束,因此拥有更大的自主权,更利于产品的竞争。

四、融资租赁在经济转型中面临极大的行业风险

融资租赁公司在运营中通常会面临信用风险、市场风险、政策风险、技术风险、法律合规风险、道德风险、操作风险等,在金融危机和通胀下的经济转型的变革中,融资租赁公司将面临更大的风险。主要有:

- (1) **面临金融危机冲击下的租金回收的风险。**世界范围内的金融危机导致我国的出口型加工业、运输业等企业受到重创,造成相当多的融资租赁公司出现租金逾期和坏账,特别是运输业的不景气,造成船舶建造业受到的冲击巨大。有的造船厂关闭,连承租人都找不到了。
 - (2) **面临市场结构调整下的行业整体萧条的风险。**我国经济转型中,必然会出现行业“扬抑发展”的现象,譬如过去一轮增长过于依赖外资和房地产,这一模式使得内资企业缺乏竞争力。全国出口的近6成和高新技术产品出口的近9成都是外商投资企业出口。而固定资产投资中增长最快的房地产本身技术含量低,带动的重化工业都是钢铁、水泥等能耗大、污染重的产业,增加了节能环保的压力。
- 更重要的是,房地产快速致富的特性打破了整个宏观资金配置的平衡,减少了本应流向技术创新、节能降耗的资金,因此,国家对这一类企业必然要压缩投资,降低规模,而如果前几年已经发生的融资租赁业务必然会遭遇巨大的风险。
- (3) **高技术产业与新兴产业中存在无序发展和“低附加值陷阱”。**有不少地方政府很热衷于发展高技术产业,不惜代价实行各种优惠政策,产业发展重点向高新技术倾斜。从实践来看,许多地方对此缺乏理性认识,更多地表现为概念的炒作、雷同式的布局、低层次的竞争、技术的盲目引进、缺乏有效的核心技术支撑等。因为无序发展带来的资源浪费和战略性发展机遇的错失,后果非常严重。以光伏产业为例,2011年末遭遇哀鸿遍野的困境,一夜之间跌到谷底。数据显示,浙江374家中小光伏企业中,至少有50%处于半停产状态,而在拉晶和切片等环节,停工的企业甚至达到70%~80%,已经破产转行的企业也不在少数,这个状况令人深思。
 - (4) **面临经济转型变革中政策变化的风险。**我国应对金融危机采取的一系列政策,已经取得了很大成效,但从经济运行的效果来看,投入产出的效率并不理想,依靠投资拉动经济增长,长期来看难以为继。过去的经济政策都是以拉动投资需求为主,没有兼顾长期问题的解决。下一步宏观经济政策在指向消费上力度会更大。我们知道,融资租赁业务最大的风险是时间的风险,融资租赁合同通常租赁期少则3~5年,多则8~10年,有的大型设备租赁标的物时间更长,如飞机、基础设施、轨道交通等,任何政策的波动都会对这类融资租赁公司的业务和租金回收带来不确定的风险。
 - (5) **面临模式创新中法律合规的风险。**在应对经济转型时,只有与时俱进、大胆创新,才能有效地规避风险。然而,在模式创新中,最大的问题是法律合规的风险,因为我国至今都没有出台《融资租赁法》,现行的法规和司法解释对业务的覆盖面又太窄,由于很多新思路、新模式没有法律依据和合理合法的解释,在实施过程中又困难重重,一旦遇到矛盾和纠纷,融资租赁公司很可能败诉。因此,融资租赁业在经济转型中要大力发展往往会遇到“两难”,处于进退维谷的境地。

五、融资租赁业必须创新和主动挑战风险

融资租赁业如何适应当前中国经济转型的需要，如何利用千载难逢的发展机遇迅速扩展自己的经营空间并有效地规避风险，唯一的道路就是大胆创新，以作为求地位，彻底改变融资租赁行业30多年来在中国地位不高，经营环境、政策环境、法律环境不善的现状。根据当前我国经济面临的难点、焦点，特别是经济转型中亟需解决的难题，从现有条件出发，通过融资租赁创新找出解决方法。而不是单纯地向政府要政策，要支持。为此，根据发达国家融资租赁的发展经验，我国的融资租赁可以有如下方面的创新。

(一) 利用融资租赁所有权和使用权分离的风险锁定特点，破解中小微企业的融资难题

中小微企业融资难是世界范围内都难以解决的难题，然而在国际上中小微企业通过融资租赁支持做强做大，甚至跨入世界巨富的例子比比皆是，我国中小微企业得益于融资租赁发展成特大型企业的也有不少，如浙江万向集团等。

融资租赁公司运作的最大特点是同时拥有物权和债权；而政府的政策性担保公司的特点是为了培植税源，会承担较大的扶持中小微企业发展的义务，且担保额度高，成本低，银行有资金，但也需要规避融资风险。如果这三类机构能联手合作，就可以共同做大。我们将这种合作称之为“按揭式融资租赁”。

按揭式融资租赁是融资租赁的一种创新，其创新思路来源于按揭式买房的成功应用，只不过这里的承租人不是个人而是中小微企业，租赁标的物不是住房而是机器设备。按揭能解决上海85%以上老百姓的购房难问题，按揭式融资租赁在解决中小微企业融资难问题上同样有着广阔的空间。

在按揭式融资租赁运作模式中，中小微企业通过租赁公司、政策性担保公司及银行的联合审查以后，就可以融资租赁的方式获得所需要的固定资产，支付20%~30%的保证金（不需要抵押），在承租期满后，设备就永久归企业所有，而租赁公司将商业银行、担保公司及设备制造商等资源整合和连接在一起，通过按揭式融资租赁购买中小微企业所需求的资产，然后以物流的形式实现资金流动，从而满足了中小微企业的融资需求。

按揭式融资租赁运作模式最大的特点是：①门槛很低。只需交付所需设备款项的20%~30%作为保证金，就可以得到100%的设备使用权。②安全性好。一旦中小微企业破产清算，将设备收回变现，即可锁定风险。

但是采用这种模式进行融资的前提是，针对中小微企业通用性较大的固定资产投资项目，并且要求中小微企业的信誉好，项目前景好，有还租能力。

中小微企业在通过租赁公司和政策性担保公司的联合审查以后，与租赁公司建立设备融资租赁关系；政策性担保公司为中小微企业提供（一般为85%~90%）履约担保；商业银行为租赁公司提供设备贷款；通用设备一般还可以由设备制造企业提供回购担保。在按揭式融资租赁运作模式中，设备制造企业通过与政策性担保公司、商业银行和租赁公司组成营销战略联盟，从而构建了一条“共享收益，共担风险”的融资租赁链，将金融、生产、贸易三者紧密结合，将银行信用、商业信用、消费信用有效叠加，尤其是利用融资租赁的所有权与使用权分离的功能，不仅使银行和担保公司锁定了风险，同时也做大了租赁公司和设备供应商，达到了多赢的格局。

按揭式融资租赁的好处有：

- (1) 对中小微企业（承租人）来说，按揭式融资租赁融资门槛低，手续简便；以融物达到融资的目的；为中小微企业开辟了一个新的、广阔的融资渠道。
- (2) 对政府部门来说，通过对按揭式融资租赁运作模式进行政策扶持，有利于解决中小微企业融资难问题，培植了税源。同时也实现了中小微企业产业转型和结构优化升级，带动融资租赁业和设备制造业的共同发展。此外，从政府担保角度而言，利用融资租赁的所有权和使用权分离的功能，由直接担保资金变成租赁物提供担保，一旦企业破产，通过收回设备并变现，锁定了风险。



- (3) 对设备制造企业来说,融资租赁可以一次性地回笼货款;可以增加客户的有效需求,加速设备的流通,扩大销售额,增加市场占有率。
- (4) 对于商业银行来说,按揭式融资租赁不仅拿到债权,也间接拿到物权。使贷款安全有了切实的保证。同时由于租赁与政策性担保的结合,租赁公司、担保公司和中小微企业,甚至供应商的信用叠加,加上按揭式融资租赁的操作办法和严格的风险防范机制,也做大了银行的中小微企业融资。
- (5) 对租赁公司来说,由于有政府政策性担保公司介入,融资问题和安全问题将迎刃而解。所有的租赁公司对中小微企业融资都会产生极大的兴趣和热情,将会启动上海乃至全国的融资租赁企业几百亿乃至上千亿的资金进入中小微企业融资。有效解决中小微企业融资难的问题。

但是,按揭式融资租赁项目运作涉及的租赁公司、担保公司、银行三者都有独立的审批机构、审批标准和审批程序,既要防范风险,又要降低门槛,也要快捷高效。减少中小微企业的负担,确实还有不少亟待解决的问题:

- (1) 评审标准、评审机构、评审方法需要统一和简化;
- (2) 交易模式、交易结构、交易流程需要统一和简化;
- (3) 企业尽调的统一和简化;
- (4) 风险共担机制的建立;
- (5) 利益共享机制的建立;
- (6) 以点带面、做强做大,市场化运作机制的建立。

(二) 融资租赁可以破解政府不动产存量资产盘活的难题

近年来,各级地方政府融资平台为拉动地方经济回升、加强基础设施建设、加快城市化建设进程发挥了重要作用。但在其迅速发展过程中,不仅形成了巨大的融资规模,加大了地方政府的偿债负担,而且蕴藏的贷款风险也正在逐渐显现。通过政府平台清理整顿后,虽然贷款风险得到抑制,但是政府融资难矛盾更加凸显,且“十二五”规划时期,各地政府投资所需配套资金落实仍是大问题。据悉地方政府投资缺口总计约34万亿元。仅浦东新区政府“十二五”规划资金缺口就有1300亿元。

如何解决这一庞大的资金需求,上海市政府提出了“创新驱动、转型发展”的思路。我们认为,通过融资租赁的创新把政府沉积的资产盘活变现,使其重新成为货币资金,可以缓解地方政府的融资难问题。当前的现状是政府和国企手上确实有大量的存量和闲置资产,巨额资金十分可惜地沉淀在这些资产中。如何盘活这些资产,成为政府吸纳社会资金,解决“十二五”规划中资金短缺的一大突破口。2010年,天津市通过融资租赁创新盘活了70多亿元的存量资产,天津空港新区政府大楼和空客厂房的售后回租报道在媒体上引起了轰动,为整个行业带来了福音。浦东新区国资委辖下的存量资产有近800亿元,如果能盘活一半存量资产,新区“十二五”规划中三分之一的资金就有了着落。显而易见,融资租赁作为现代服务业的一支生力军对于上海经济的发展具有巨大的推动作用!

然而我们在实践中碰到“两难”问题。一方面,融资租赁售后回租的基本要约是租赁的标的物必须首先进行所有权过户,不过户合同就无效;另一方面,合同一旦过户,就会产生大量的税费,尤其是政府的存量不动产物业大多是政府划拨土地,过户中的土地出让金补缴额就是一个天文数字。要解决这些问题,我们必须逾越五大关键障碍:

- (1) 必须解决合同过户的法律障碍;
- (2) 必须解决补缴土地出让金等税费障碍;
- (3) 必须会同法律、税务、银行、政府等相关部门共同设计能够规避法律、税费,锁定风险的融资租赁创新方案;
- (4) 必须让银行的合规部门及监管部门理解、接受、支持貌似有“法律瑕疵”的创新方案;
- (5) 必须让租赁公司的法务部门和董事会理解、接受、支持貌似有“法律瑕疵”的创新方案。

当然,最大的障碍是交易模式中的安全性问题,我们通过嫁接国资委直属的经营性集团公司的信用或土地等不动产抵押等信用较好地解决了这些问题。可以确信,一旦这种模式可行,必将对浦东和上海的经济推动及“四个中心”建设产生重大的影响,必将给上海现代服务业的发展及形成新的现代服务业产业群带来实质性的突破和推动。

(三) 融资租赁可以破解西部资金短缺的重大命题

上海作为中国的金融中心和制造中心，拥有巨大的生产能力。但是，企业生产过剩、销售不畅的现象也在一定程度上存在。上海目前仅设备积压就有几千亿元人民币，找不到销售渠道只能“睡大觉”，可供租赁的资源不计其数，是一个庞大的租赁供方市场。许多质量优异的设备不是没有需求，而是营销方式单一，有效需求少。

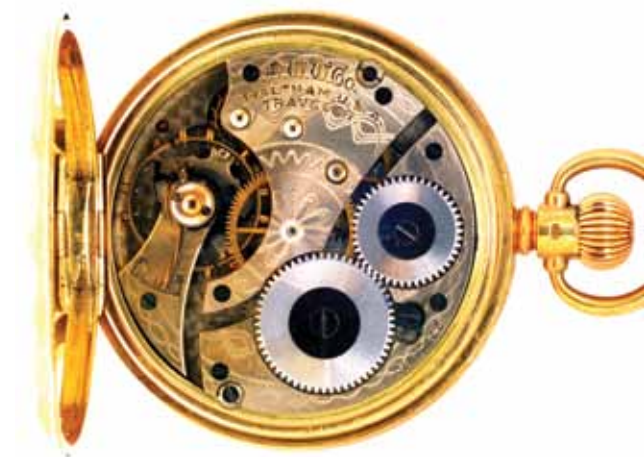
与此形成强烈反差的是，西部地区的经济发展急需各种设备投入。仅重庆地区在企业结构调整、农副产品加工与农业产业化、城市综合开发建设、生态环境保护与建设等方面急需上马的效益好、建设周期短的项目所需资金近千亿元，西部地区目前最缺乏的是资金、技术、人才和设备资源等，首当其冲的就是资金。许多西部企业不是不想到东部地区来购买设备，而是缺乏资金，而东部企业也急于开拓西部市场，但是仅仅依靠一次性销售的方式很难打开市场。创新融资租赁的优势就在于，让西部企业实现用明天的钱办今天的事，并通过市场运作和盈利，逐年偿还租金，避免了固定资产投资中的大量资金沉淀，降低了资本运营成本，而东部企业则通过以租代售大大拓展了销售。因此，创新租赁可以让东西部的资源有效地实现对接。

融资租赁创新必须将银行信用、商业信用、企业信用进行有效叠加，设计出“嫁接信用、分担风险、多家共赢”的创新租赁模式，立足上海及东部地区等经济发达地区的综合优势及庞大的设备供应市场，依托政府和金融机构的支持，依靠厂商联盟、银企合作的强大资源平台，积极拓展西部庞大的租赁需求市场。以融物达到融资的目的，以物为载体实现物流、资金流、信息流的“三流合一”，有效地拉动内需，冲破金融壁垒，实现东资西调。

六、融资租赁业深层次问题亟待解决

融资租赁虽然功能强大，对转型中的中国经济有着巨大的推动作用，但是目前仍旧发展缓慢，究其原因，有如下深层次原因需要重视并予以解决：

- (1) 迅速转变观念。尤其是政府主管部门要加强学习、转变观念，这是推进融资租赁市场发展的前提；要全面认识大力发展融资租赁市场的意义；要转变重所有权、轻使用权的陈旧观念；要认清大力发展融资租赁市场对中国经济转型的挑战与机遇。
- (2) 迅速改变我国融资租赁业多头监管、政出多门的现状。目前由银监会监管金融租赁公司，由商务部监管中外融资租赁公司和内资租赁公司。融资租赁缺乏统一的行业管理，没有统一的协调管理机构，这为融资租赁市场的继续发展留下了隐患，不利于统一的政策指导和制定全行业发展规划。
- (3) 尽快完善融资支持政策。拓宽融资渠道，充实融资租赁公司的资金来源。一方面，在政府支持下，由银行向融资租赁公司提供低息贷款，使融资租赁公司获得低息信贷资金。另一方面，适当扩大融资租赁公司的资金来源，对实力雄厚、信誉良好、业绩突出的融资租赁公司，允许通过发行债券和股票从资本市场进行直接融资。允许对租赁资产进行交易和变现。
- (4) 迅速加强租赁公司的整体管理水平，提升我国融资租赁公司的市场占有率和国际竞争力，提升融资租赁公司的风险管理、财务管理和资产管理能力。



2013年中国保险业 十大趋势与展望（上）

2012年，全国保费收入达1.55万亿元，同比增长8%。其中，财产险保费收入为5,331亿元，同比增长15.4%；寿险保费收入为8,908亿元，仅取得2.4%的增长；健康险保费收入为863亿元，同比增长24.7%；人身意外险保费收入为386亿元，同比增长15.6%。相比较2011年财产保险增长18.5%，人身险增长6.8%，不论产险和寿险，其增长速度均进一步放缓，也远低于2001~2010年十年间平均复合超过20%的增长比率。

2012年，投资回报下跌和退保增加继续困扰着寿险行业；汽车销售量低增长、费率下跌，以及渠道费用的上升也使产险行业担心承保利润的高峰是否已经过去。

截至2012年末，保险业资产总额达7.4万亿元，较年初增长22.9%，但令保险业人士感觉到危机的是，2012年末中国信托行业管理资产规模已经超过7.5万亿元，成功超越保险行业。保险行业的资产规模不但落后于银行和证券行业，甚至比不上5年前规模只有保险行业20%的信托行业。

古人说：“穷则变，变则通。”2012年，改革转型的呼声不绝于耳。保险行业不断探索投资渠道的开放、销售模式的转变，以及产品定价，甚至偿付能力监管等方面的改变。我们选取了未来2~3年对中国保险业发展最具影响力的十大前沿话题，总结2012年的发展，展望未来的趋势。

一、投资渠道大开放，大资产管理时代来临

2012年6月，中国保险监督管理委员会（以下简称“保监会”）在大连召开了保险投资改革创新的闭门会议（业内人士称为“大连会议”），并在会议上讨论了13项投资新政征求意见稿，掀起了险资运用创新的大潮。

近年来，保监会逐步放开了在保险业资金运用领域的一些限制，当中涉及股票、证券投资基金份额、基础设施债权计划、未上市股权投资、无担保债券和不动产等。尽管如此，保险公司在资金运用时仍然受限较多，与国际成熟市场相比，国内保险投资资产类型较少、范围有限，这也是导致中国保险业整体投资收益率较低的原因。对于投资类型的寿险产品，面对低迷的股市，以及其他投资范围比较广泛的信托或理财产品，缺乏竞争能力。之前，我们研究了近年保险资金运用的开放趋势，并特别指

出未上市股权投资和不动产投资是我们比较关心的发展重点。但是，在2012年，保险资金渠道拓宽政策的步伐超出了我们，甚至整个保险行业的预期。

保监会在大连会议中一次性下发了13项保险投资规定的征求意见稿，内容涉及允许保险机构委托证券公司和基金公司管理保险资金、参与金融衍生品交易、拓宽保险资金境外投资品种和范围、拓宽境内股权和不动产投资范围、开展股指期货业务等内容。一名业内资深人士表示，13项新政的内容只有4项过去略有风声，其他9项政策的推出超出业内人士预期。

7月，保监会落实第一批的4项政策，这第一批新政主要包括保险资金管理委托资格的开放，债券投资、股权和不动产投资的拓宽；并在10月份继续稳步落实6项政策，第二批包括容许保险公司投资理财产品、信贷资产产品、使用衍生工具（包括股指期货）、明确债权计划投资范围（见表1）。截至年末，旨在拓宽投资渠道的13条新政已经正式推出10条。根据媒体报道，尚未正式发布的应该还包括《保险机构融资融券管理暂行办法》、《保险资产托管管理暂行办法》及《关于加强保险资金公平交易、防范利益输送的通知》。

根据《保险资金委托投资管理暂行办法》，险资可委托的投资人已扩大到证券公司和基金公司。截至2012年末，共有40家企业取得了保险资金管理的资格（见表2），未来的竞争肯定远远超过过去只有10多家保险资产管理公司的局面。另一方面，保险资产管理公司在符合相关监管规定后，将可以开展公募基金管理业务。

对于这种资产管理竞争加剧的趋势，保险资产管理公司并非没有顾虑。某保险资产管理公司高管表示，保险资产管理公司主要以服务系统内保险公司为主，第三方机构资产管理的占比比较低，也没有服务个人客户的经验，市场化程

文启斯
德勤中国
保险行业领导合伙人

王锦
德勤中国
金融服务行业管理咨询合伙人

杨桦
德勤中国
金融服务行业管理咨询副总监

度不如证券、基金和信托行业。投资领域最注重人才，但国内保险资产管理公司的薪酬激励机制无法和支付核心人员动辄数百万元甚至上千万元年薪的证券或基金管理行业竞争。

对于投资产品的开放，不少保险业的高层表示他们在13项新政中最关注《关于保险资金投资有关金融产品的通知》，因为该通知将容许保险公司投资信托产品、银行理财产品和券商集合理财产品。虽然通知对于产品的评级和流动性等设置了较多的限制，但由于信托产品和理财产品本身具有一定的规模，符合资格、可供保险公司选择的产品还是具有一定的数量。

部分保险公司则对《对于保险资金参与股指期货交易规定》感兴趣，并指出保险公司将可使用股指期货对冲市场风险。因此，继先前部分保险公司已获准使用利率互换来对冲利率风险，股指期货的使用将进一步增加保险公司风险管理的能力。

但是，对于国外资产管理行业非常感兴趣的《保险资金境外投资管理暂行办法实施细则》，部分保险公司则表示暂时不在日程上。某保险公司高管表示，对于境外投资，他们相对并不熟悉，现在出现了众多新的投资渠道，他们重点研究的是比较熟悉的国内金融产品。此外，由于国内保险公司负债主要还是以人民币为主，而且近期人民币对美元还是呈现升值的趋势，因此海外投资还需要考虑汇兑风险。

这一系列保险投资新政几乎已囊括了保险行业所有能预期的投资渠道和投资工具，并普遍地降低了保险公司偿付能力的要求，对于容许参与这些新投资渠道的保险公司，偿付能力充足率要求就从过去的150%往下调整到120%。此外，对于相关投资的多项比例也获得开放，如无担保非金融企业债券占总资产的比例上限由原先的20%提高至50%。

部分规模较小的保险公司反映，在各项新政中，除了对资金管理机构（包括保险资产管理公司）有多项要求外，保险公司本身也需要聘用一定数量的相关专业人才，这对于规模比较小的保险企业还是产生比较大的压力。一些规模较小的保险公司表示，当初设立资产管理公司时，已经把投资人员分离至资产管理公司，现在需要增加聘用投资人士满足监管规定，也是一项重大的投资。

面对这一系列的新政，我们预计保险企业的投资范围必然会变得更广泛，且投资回报也会获得提升。但同时，保险企业面临着新渠道投资所带来的风险。就以保险公司最感兴趣的理财产品、信托产品投资，以及衍生工具的运用为例，不少投资人士指出近期一些理财产品、信托产品暴露出越来越多的兑付风险，保险资金必须非常慎重；至于衍生工具的错误运用产生的风险在全球金融市场的历史中更是俯拾即是。此外，我们也关心新投资渠道带来的会计核算和税务风险。

此外，保险行业的资产管理公司面对证券行业、基金管理行业的竞争，也已经准备好在各方面提升自己，这包括全面拓展各项新政容许的投资范围，形成“更大更全”的资产管理公司。部分资产管理公司已经开始全面检讨部门的设置、人才配置、风险管理，薪酬体系，甚至后台营运设计。我们预计保险资产管理公司在2013年必定秣马厉兵，迎接“大资产管理时代”下“多产品、多市场、多类型”的运作模式。



表1 2012年投资新政出台进展表

阶段	日期	事件	主要内容
准备阶段	4月27日	保监会主席浙江温州调研	<ul style="list-style-type: none"> 要求进一步深化保险资金运用市场化改革，积极探索保险资金服务实体经济的新模式和新路径。
	6月11-12日	大连会议召开，13项保险投资新政（征求意见稿）出台	<ul style="list-style-type: none"> 保监会下发的保险投资规定征求意见稿中，包括允许保险机构开展融资融券业务、参与境内及境外金融衍生品交易、拓宽保险资金境外投资品种和范围、拓宽境内股权和不动产投资范围等13项内容。
第一阶段	7月19日	保监会发布《保险资金投资债券暂行方法》	<ul style="list-style-type: none"> 容许保险公司投资混合债券和可转债投资。 无担保债投资评级限定由AAA级降为AA级及以上。 放宽发行限制，除公开招标方式以外，增加了符合规定的簿记建档方式。大部分以簿记建档方式发行中期票据将符合资格。
	7月23日	保监会发布《保险资金委托投资管理暂行办法》	<ul style="list-style-type: none"> 首次容许证券公司、证券资产管理公司和基金管理公司向保监会申请成为保险资金投资管理机构。 证券公司、证券资产管理公司或基金管理公司要成为保险资金的受托投资机构，需要取得客户或特定客户资产管理业务资格三年以上。 对于证券公司、证券资产管理公司，最近一年客户资产管理业务管理资产余额（含全国社保基金和企业年金）不低于100亿元，或者集合资产管理业务受托资金余额不低于50亿元。 对于基金管理公司，最近一年管理非货币类证券投资基金余额不低于100亿元。
	7月25日	保监会发布《关于保险资金投资股权和不动产有关问题的通知》	<ul style="list-style-type: none"> 明确或调整了《保险资金投资不动产暂行办法》、《保险资金投资股权暂行办法》。 不动产投资仍然限于商业/办公不动产、保险相关的养老、医疗和汽车不动产，以及自用不动产，但明确可间接投资公共租赁和廉租住房。 直接股权投资从保险类企业、非保险类金融企业和与保险业务相关的养老、医疗、汽车服务等企业的股权，拓展至能源、资源和保险相关的现代农业、新型商贸流通企业的股权；明确可间接投资成长基金、并购基金、新型战略产业基金。 取消了保险公司上一会计年度盈利要求；净资产要求从10亿元下调为1亿元。
	7月27日	保监会发布《保险资产配置管理暂行办法》	<ul style="list-style-type: none"> 要求投连险、变额年金、养老相关产品及财险非预定收益投资性产品设置独立账户，自主决定资产配置比例和结构。

阶段	日期	事件	主要内容
第二阶段	10月22日	保监会发布《关于保险资产管理公司有关事项的通知》	<ul style="list-style-type: none"> 明确保险资产管理公司可以受托管理养老金、企业年金、住房公积金等机构的资金和能够识别并承担相应风险的合格投资者的资金。 容许资产管理公司以资产管理产品或专户名义进行资产管理。 容许资产管理公司向有关金融监管部门申请，依法开展公募性质的资产管理业务。 资产管理公司可以按照有关规定设立子公司，从事专项资产管理业务。
	10月22日	保监会发布《关于保险资金投资有关金融产品的通知》	<ul style="list-style-type: none"> 容许保险公司投资理财产品、信贷资产；支持证券、集合资金信托计划、专项资产管理计划和项目资产支持计划，但投资账面余额合计不得高于保险公司上季末总资产的30%；投资基础设施和不动产合计不超过20%。 理财产品投资范围限于境内市场的信贷资产、存款、货币市场工具及公开发行且评级在投资级以上的债券，且基础资产由发行银行独立负责投资管理，自主风险评级处于风险水平最低的一级至三级。发行银行上年末经审计的净资产应当不低于300亿元人民币或者为境内外主板上市商业银行，信用等级不低于国内信用评级机构评定的A级；境外上市并免于国内信用评级的发起银行，信用等级不低于国际信用评级机构评定的BB级。 信贷资产支持证券，入池基础资产限于五级分类为正常类和关注类的贷款。产品信用等级不低于国内信用评级机构评定的A级。发起机构的银行业金融机构的要求和理财产品相同。 集合资金信托计划，基础资产限于融资类资产和风险可控的非上市权益类资产，且由受托人自主管理，承担产品设计、项目筛选、投资决策及后续管理等实质性责任。固定收益类的集合资金信托计划，信用等级应当不低于国内信用评级机构评定的A级。担任受托人的信托公司上年末经审计的净资产不低于30亿元人民币。 专项资产管理计划，信用等级不低于国内信用评级机构评定的A级。担任计划管理人的证券公司上年末经审计的净资产应当不低于60亿元人民币，证券资产管理公司上年末经审计的净资产不低于10亿元人民币。
	10月22日	保监会发布《基础设施债权投资计划管理暂行规定》	<ul style="list-style-type: none"> 明确偿债主体为项目方或其实际控制人，具备担任融资和偿债主体的法定资质；具有稳定可靠收入和现金流，财务状况良好；信用状况良好，无违约记录；还款来源明确、真实可靠，能覆盖债权投资计划的本金和收益等。 债权投资计划的项目方资本金不低于项目总预算的30%或者符合国家有关资本金比例的规定，在建项目自筹资金不低于项目总预算的60%。保监会还专门确定了有效的信用增级方法。 债权投资计划需要依规注册或备案，并在符合条件的金融资产交易场所发行，实现受益凭证的登记存管和交易流通。

阶段	日期	事件	主要内容
第二阶段	10月22日	保监会发布《保险资金境外投资管理暂行办法实施细则》	<ul style="list-style-type: none"> 容许投资于45个发达国家和部分新兴市场国家/地区的货币市场工具、权益工具、固定收益证券、股权、不动产、基金和衍生工具等。保险资金可直接投资于未上市企业股权，但限于金融、养老、医疗、能源、资源、汽车服务和现代农业。直接不动产投资限于具有稳定收益的成熟商业和办公不动产。
	10月23日	保监会发布《保险资金参与金融衍生产品交易暂行办法》	<ul style="list-style-type: none"> 允许保险机构（包括保险集团公司、保险公司和保险资产管理公司）在以对冲或规避风险为目的的前提下参与境内衍生品交易，包括远期、期货、期权和互换（掉期）。
	10月23日	保监会发布《保险资金参与股指期货交易规定》	<ul style="list-style-type: none"> 允许保险机构选取成立5年以上，上季末净资本达到人民币3亿元（含）以上，且不低于客户权益总额的8%的期货公司来参与境内股指期货交易。 规定要求卖出股指期货合约价值，不得超过其对冲标的股票及股票型基金资产的账面价值。

表2 2012年获准管理保险资金资格的机构名单

阶段	日期	数量	具体名单
第一批	9月19日	9家	博时基金、大成基金、华安基金、海富通基金、华泰柏瑞基金、嘉实基金、诺安基金、海通证券、中国国际金融
第二批	10月12日	17家	长城基金、富国基金、广发基金、国海富兰克林基金、华宝兴业基金、华夏基金、建信基金、南方基金、鹏华基金、上投摩根基金、招商基金、东方证券、光大证券、国泰君安、招商证券、宏源证券、中信证券
第三批	10月23日	14家	长盛基金、工银瑞信基金、国泰基金、汇添富基金、交银施罗德基金、融通基金、泰达宏利基金、易方达基金、银华基金、中海基金、中银基金、泰康资产管理、长江证券、广发证券

文启斯

德勤中国
保险行业领导合伙人

俞佳

德勤中国
金融服务行业企业风险
管理助理经理

二、资本市场持续疲软，2013是否回暖？

作为资本市场的重要参与者，保险业的发展深受资本市场走势的影响。2012年，中国经济延续了发展放缓的疲软势头，央行两次降息，并于7月6日实施不对称降息，一年期存款基准利率下调0.25%，一年期贷款基准利率下调0.31%。调整后，中国金融机构一年期存贷款基准利率已分别降至3.00%和6.00%；两次下调存款准备金率，中国大型金融机构目前执行20%的存款准备金率。

股市方面，沪深股市继续延续了2011年的疲弱表现（2011年，上证指数下跌28.41%，深证成指下跌21.68%）。其中，上证指数接连下挫，一度探底至1949.46点，尽管在年末出现大幅反弹，但纵观全年涨幅仅有3.17%，深证成指涨幅也仅为2.22%，两地股市表现分列全球主要市场末流（见表3）。连续两年的股市低迷对保

险业的影响也充分反映了和国际上其他的保险公司比较，资产配置中股权投资比例较高所蕴含的风险。如果不考虑投资连接产品账户资产（这些资产的市场风险由保户全面承担），在其他地区，保险公司一般股权投资的配置少于5%。在中国，根据2012年半年报，上市保险集团的股权投资比例最低是7%，最高的约14%，简单平均也达到10%以上。

债市方面，2012年12月末中债综合指数（净价）为100.75点，较上年同期的101.25点下降0.49%。其中，利率债及高等级信用品种全年震荡走弱，利率曲线一度整体下跌，但在下半年回升。总结全年，国债收益率整体上升，但国债和信用债之间的利率收窄。年中也曾发生山东海龙、江西赛维等发债主体兑付危机，但经地方政府介入而化解。

表3 2012年中国主要股市行情

	2012-1-4	2012-3-30	2012-6-29	2012-9-28	2012-12-31
上证综指	2,169.39	2,262.79	2,225.43	2,086.17	2,269.13
深证成指	8,695.99	9,410.26	9,500.32	8,679.22	9,116.48
恒生指数	18,727.31	20,555.58	19,441.46	20,840.38	22,656.92

数据来源：新浪财经，2012年。

表4 债券收益率情况一览表

品种	年期	2012-1-4	2012-3-31	2012-6-29	2012-9-29	2012-12-31
银行间国债	5年期	3.05%	3.12%	2.91%	3.17%	3.22%
	10年期	3.44%	3.50%	3.33%	3.46%	3.57%
银行间固息企业债 (AAA)	5年期	4.90%	4.76%	4.24%	4.73%	4.96%
	10年期	5.18%	5.15%	4.99%	5.12%	5.29%
银行间固息企业债 (AA+)	5年期	5.85%	5.72%	4.90%	5.48%	5.49%
	10年期	6.09%	6.10%	5.70%	5.82%	6.00%
银行间固息企业债 (A)	5年期	9.85%	10.43%	9.18%	9.61%	9.54%
	10年期	9.75%	10.69%	10.32%	10.47%	10.43%

数据来源：中国债券信息网。

股市和债市的动荡直接影响着人寿保险公司的业绩。保险公司的投资资产主要分为可供出售金融资产和持有至到期投资。可供出售金融资产以公允价值计量，但公允价值变动仅反映为权益变动，不影响利润表。但是，2011~2012年，资本市场持续低迷，根据《企业会计准则第22号——金融工具确认和计量》的规定，对于权益工具，公允价值发生严重或非暂时性下跌是其中一种减值的客观证据。一旦出现减值，这些浮亏必须反映于利润表。准则及解释均未明确规定“严重或非暂时性下跌”的具体标准。

据上市保险公司2012年三季报显示，四大上市险企（不包括仅在香港上市的人保财险，人保财险仅编制了半年报）前三季度计提资产减值损失累计已超过450亿元。其中，中国太保、中国平安、新华保险及中国人寿第三季度计提资产减值准备分别达16亿元、26亿元、28亿元及139亿元（没有考虑影子调整和递延税的影响）。中国人寿甚至因为过百亿元的减值损失导致了自上市以来首次出现季度亏损。

由于目前寿险公司主要销售投资性产品，投资回报的下滑和其他金融机构的竞争威胁，导致寿险公司最主要的利润驱动因素——利差收益收窄，甚至可能产生更多的退保。2012年受困于市场行情不理想，分红、万能等投资类产品的吸引力下降，寿险公司的保费收入增速明显放缓，银保渠道退保潮频现。

2011年，我们指出“资本市场的波动还是会在2012年的上半年影响寿险公司的销售和退保。但由于股市已经连续两年下调，债市也在2011年度第4季度回升，资本市场对保险公司的负面因素能否在2012年慢慢消除，是需要进一步观察的”。不幸的是，资本市场的波动对寿险公司的负面影响远远超出了我们的预期。可喜的是，经历了2012年12月股市的超过14%的大幅度反弹后，2013年1月上证指数在2200~2400点波动。目前投资者对2013年的资本市场表现出谨慎乐观的态度，但股市对保险企业经营状况波动性的影响还将持续。

2013年全国保险监管工作会议指出，“寿险公司退保金达1198亿元，退保率为2.76%，低于5%的警戒线”。可是，业内人士担心，收入下跌，退保增加，加上满期给付的压力，会对一些规模较小的寿险公司产生巨大的流动性风

险。某保险高管甚至断言：“2013年，部分寿险公司的流动性风险远高于偿付能力不足的风险。产生困难的寿险公司可能表面上的偿付能力还是非常充足的。因此，流动性监管才是未来的关注重点。”这是危言耸听？还是警世良言？视乎低迷的资本市场在2013年何时才能改善。

三、次级债发行创新高，偿付能力压力有所缓解

由于保险业务的高速发展和资本市场的低迷，偿付能力充足率一直困扰整个保险业。就2012年中期与2011年末比较，由于寿险业务增长放慢，加上各项融资活动，寿险公司的偿付压力有所减轻；反之，除了人保财险，上市的产险公司的偿付能力面临较大的压力。

2012年上半年，人保财险在保费收入同比增长约10.7%，再保险分出比例从2011年的21.5%下跌至14.5%的情况下，仅靠当期利润和可供出售金融资产公允价值的回升，保持了偿付能力的水平。几家较大的上市保险公司偿付能力变化情况见表5。

表5 主要上市保险企业偿付能力充足率的变化

	2012 年中期	2011 年	2010 年	2009 年
中国人寿	231%	170%	212%	304%
人保财险	184%	184%	115%	111%
人保寿险	136%	132%	124%	181%
人保健康险	101%	107%	115%	211%
平安产险	164%	166%	180%	144%
平安寿险	167%	156%	180%	227%
太保财险	194%	233%	167%	173%
太保寿险	183%	187%	241%	208%
新华人寿	159%	156%	35%	36%
太平寿险	169%	178%	270%	222%

数据来源：各保险公司年报、中期报告和人保集团招股书。

文启斯
德勤中国
保险行业领导合伙人

俞佳
德勤中国
金融服务行业企业风险管理助理经理

正如我们之前指出，保监会于2011年修订的《保险公司次级定期债务管理办法》大幅度提高了募集次级债的门槛，对募集规模的上限由不超过上年末净资产的100%降低到50%，使得次级债发行作为偿付能力的手段受到限制。此外，该办法也不容许集团公司发行次级债（但2013年初提出修订，将容许集团公司再次发行次级债）。公开数据显示，人保财险和太平人寿需要在股东补充资本后，才可以发行新的次级债，这将大大增加股东注资的压力，尤其是部分过去发行的次级债即将到期的保险公司。2011年，人保财险集资50亿元，开了国有保险企业上市后再融资的先例。2012年，我们注意到泰康人寿也在补充资本金20亿元。

保监会的数据显示，2012年共有12家公司获批发行次级债，总额达到991亿元（见表6），超过了上年的577亿元，而实际发行额为711亿元，也高于上年的600亿元。当中募集超过100亿元的包括于2011年实现A+H上市、融资逾百亿元的新华保险，2011年首次发行次级债的中国人寿，以及平安集团260亿元的A股次级可转换公司债券。平安的次级可转换公司债券更是次级债的新品种，受惠于2012年5月31日保监会正式发布的《关于上市保险公司发行次级可转换债券有关事项的通知》。经过2012年的次级债发行后，我们估算，不少保险企业如太保寿险和新华人寿等也开始逼近50%的底线。

表6 2012年保险公司/集团次级债发行获批准情况

获批日期	发债保险公司	获批金额上限	期限
2012-4-10	平安寿险	90亿元	10年期
2012-4-27	阳光财险	10亿元	15年期
2012-5-17	平安保险（集团）	260亿元	A股次级可转换公司债券
2012-6-25	中国人寿	380亿元	10年期和15年期
2012-6-25	新华人寿	100亿元	10年期
2012-8-3	太保人寿	75亿元	10年期
2012-8-14	国寿财险	20亿元	10年期
2012-8-14	中英人寿	10亿元	10年期
2012-8-29	华泰人寿	7亿元	10年期
2012-11-26	光大永明人寿	9亿元	10年期
2012-12-20	平安产险	30亿元	10年期

数据来源：保监会网站业务公告数据。获批金额上限为人民币。



除发行债券外，其他募集资金方式包括通过上市融资、股东注资等手段补充资本金。2012年，人保集团在港交所上市募资276亿港元，募集资金大部分用在提高偿付能力充足率上，缓解资本补充的压力。根据保监会数据，2012年全年46家保险公司获批准增加注册资本，涉及金额约636亿元，低于2011年900亿元。关于重大的保险企业注资事项，请参考表7。

面对保险企业持续攀升的融资需求，自2011年年底以来，监管层不断释放“完善保险公司的资本补充机制”信号。保监会主席项俊波在2012年初的全国保险监管工作会议上表示，鼓励公司适时通过多种渠道补充资本，缓解偿付能力压力。同时，由于《商业银行资本管理办法（试行）》的出台，银监会加快了对包括优先股、含减记或转股条款的混合资本工具等在

内的商业银行创新资本工具的研究；并于2012年12月7日发布《中国银监会关于商业银行资本工具创新的指导意见》（56号文）。我们预计保险业有可能借鉴商业银行创新资本工具的开闸，进一步拓宽资本补充的渠道。

继放行可转债之后，2012年7月，保监会下发《关于人身保险公司使用再保险改善偿付能力有关事项的通知》的征求意见稿，明确提出人身险公司可以通过使用再保险来改善偿付能力，并规范认可的再保险安排。

除了发行次级债、股东注资和再保险以外，尚有保险公司通过改变会计政策加强或保护偿付能力，当中最主要的包括了投资性房地产的核算从成本模型改为公允价值模型，使位置优良的出租房产的市场价值得以合理反映，并提升了账面资产总值；另一种手段是当预期利率上

表7 2012年获批增资超过10亿的商业保险企业和集团

注资日期	保险公司	注资背景	注资金额
2012-3	中国人寿再保险	注册资本增至57.2亿元人民币	15亿元
2012-5	光大永明人寿	注册资本增至42亿元人民币	12亿元
2012-6	中国财产再保险	注册资本增至85.3亿元人民币	10亿元
2012-7	天安保险	注册资本增至56.5亿元人民币	13亿元
2012-8	中邮人寿	注册资本增至20亿元人民币	15亿元
2012-8	民生人寿	注册资本增至60亿元人民币	20亿元
2012-10	工银安盛人寿	注册资本增至37.1亿元人民币	15亿元
2012-11	太保集团	完成向新加坡政府、挪威银行和阿布达比投资局的定向增发	104亿港元
2012-3 2012-11	中华联合保险	3月保险保障基金向中华联合首轮增资60亿元；11月东方资产债转股方式注资78.1亿元	138.1亿元
2012-11	嘉禾人寿	农业银行收购嘉禾人寿，嘉禾人寿以每股2.5元的价格向农业银行定向增发10.36亿新股	25.9亿元
2012-6/11	生命人寿	以转增资本方式，注册资本增至107.7亿元人民币	34.4亿元
2012-11	合众人寿	注册资本增至27.8亿元人民币	10.5亿元
2012-12	泰康人寿	注册资本增至28.5亿元人民币	20亿元
2012-12	民安财产保险	注册资本增至20亿元人民币	10.1亿元
2012-12	和谐健康保险	注册资本增至21亿元人民币	11亿元
2012-12	正德人寿	注册资本增至20亿元人民币	10亿元
2012-12	信达财产保险	注册资本增至30亿元人民币	20亿元
2012-12	人保集团	上市全球发售68.98亿股H股	276亿港元

数据来源：保监会网站业务公告数据及各保险公司公告。除特别注明外，注资金额为人民币。

文启斯
德勤中国
保险行业领导合伙人

卢展航
德勤中国
保险与精算服务
合伙人

张 强
德勤中国
金融服务行业管理
咨询总监

升，债券的公允价值未来将会下跌时，将部分债券以公允价值计量的可供出售金融资产转为摊余成本计量的持有至到期投资。

自从2009年财政部颁布《保险合同相关会计处理规定》以来，保险公司，特别是寿险公司盈利能力显著提升，可是偿付能力没有得到相应的改善。很多保险行业以外的人士并不理解有关的原因，这是因为在财务报告和偿付能力报告中，寿险公司的主要负债，即寿险/健康险责任准备金，计算所采用的评估方法和假设并不一致。偿付能力报告还是沿用过去的监管体系，计算准备金使用的假设相对比较保守，评估的准备金比财务报告中的准备金要高。

2012年，尽管股市低迷，次级债的大规模发行使保险行业偿付能力压力有所缓解，但我们 also 见证了人保集团的总体上市和太保集团的定向增发。2013年，我们预计已发行较大金额次级债的保险公司仍然将面临较大的融资压力。

四、偿付能力改革展开，争取3~5年完成

之前我们指出“中国偿付能力沿用欧洲偿付能力旧有制度，是否需要改革，如何改革，过去几年也是争论不休的话题……中国保险业偿付能力标准监管委员会在2011年10月的换届选举

中，有更多的技术人员入选，委员会也首次引入了任职于会计和精算咨询机构的专业人士。我们期望在2012年保监会对偿付能力改革提出更多建设的思路”。2012年，中国偿付能力监管标准终于揭开了改革的序幕。

2012年4月18日，保监会召开了第二代偿付能力监管制度体系（以下简称“偿二代”）建设启动会，决定以3~5年的时间完成中国偿付能力的改革。环顾全球，目前欧盟偿付能力II经过多轮量化测试后进入最后阶段，美国偿付能力监管现代化工程也一直在进行；在亚洲，新加坡、韩国和中国台湾也采用了风险资本的概念，我们沿用的欧盟偿付能力I显得相对落后。

对于整个偿付能力改革的进程，截至2013年2月末，保监会一共发布了16期的工作简报。这些工作简报报道了中国偿付能力改革的一些重要会议内容，也包括了国外偿付能力发展的最新动向，如欧盟偿付能力II，美国的偿付能力现代化、新加坡、澳大利亚和韩国等地的偿付能力监管。从这些简报中，我们能对2012年的整个过程有比较完整的理解。

保监会发布的第2期工作简报明确指出，整个偿付能力改革将分为5个阶段进行。同时，保监会将筹建13个工作小组，研究应对改革过程中的各项问题。



图1 偿二代发展路径预测

第一批启动项目组	1	全面总结项目组一	评估现行标准是否符合我国实际
	2	全面总结项目组二	比较现行标准、欧盟偿付I、II和美国风险资本制度
	3	整体框架项目组	细化三支柱框架的具体范畴和制度内容
	4	最低资本——产险承保风险项目组	设计产险承保风险最低资本要求标准
	5	最低资本——寿险承保风险和利率风险项目组	设计寿险承保风险和利率风险最低资本要求标准
	6	最低资本——资产风险项目组	设计资产风险最低资本要求标准
尚未启动项目组	7	全面总结项目组三，比较分析保险业与其他金融行业（银行业、证券业）的资本要求	
	8	最低资本——其他风险和风险相关性项目组	11 逆周期监管项目组
	9	实际资本项目组	12 第二支柱项目组
	10	集团监管项目组	13 第三支柱项目组

图2 偿二代13个项目组分工



按照各期的工作简报，我们对各工作小组的进度理解如表8所示。

表8 偿二代工作小组进度

全面总结 项目组一及 项目组二	7月10-12日	<ul style="list-style-type: none"> 汇报了项目组工作思路、工作进展和项目测试方案（建议稿）。
	8月24日	<ul style="list-style-type: none"> 向偿付能力监管标准委员会汇报测试方案。
	9月25日	<ul style="list-style-type: none"> 保险公司进行全面总结项目定量测试培训。
	10-11月	<ul style="list-style-type: none"> 项目组对参与测试的公司报送的数据进行了汇总、分析和比较。
	12月	<ul style="list-style-type: none"> 完成了研究报告初稿。
总体框架	4月	<ul style="list-style-type: none"> 对国际保险监督官协会保险监管核心原则、欧盟、美国及其他具有代表性的偿付能力监管模式、标准、方法和具体规定进行了系统研究，提出初步思路。
	7月20日	<ul style="list-style-type: none"> 偿二代领导小组办公室确定了整体框架思路和原则，在此基础上形成初稿。
	12月	<ul style="list-style-type: none"> 经多次在不同层次和不同范围进行讨论修订，形成了征求意见稿。
寿险承保风险 及利率风险 项目组	7月10-12日	<ul style="list-style-type: none"> 完成了寿险承保风险和利率风险的理论及实证研究，确定了寿险承保风险的内容及维度。 讨论了项目组工作思路、工作计划以及利率风险、资产负债评估原则、监管准备金和会计准备金等重点问题，并对该项目组与资产风险项目组的关联问题进行了研究，包括收益率曲线外推、情景生成等问题。
	11月13日	<ul style="list-style-type: none"> 10家保险公司参与了量化工作的培训。
	12月	<ul style="list-style-type: none"> 完成参与测试公司的数据汇总和结果分析工作。
资产风险 项目组	7月10-12日	<ul style="list-style-type: none"> 完成资产风险最低资本标准的国际比较研究，重点对美国、欧盟资产风险分类标准、计量方法及资本要求进行了对比分析。 梳理了国内保险公司现有投资资产类别、品种，提出了资产风险细分建议。 会议中确定市场集中度风险从第一支柱调整至第二支柱。
	12月	<ul style="list-style-type: none"> 形成了较成熟的资产风险计量模型和测试方案，待提交偿二代领导小组办公室审议。
产险承保风险 项目组	7月10-12日	<ul style="list-style-type: none"> 分析了美国、欧盟、澳大利亚和我国现行标准产险承保风险资本要求的差异。 提出了具体的计量模型和方法建议，并梳理了产险承保风险最低资本标准制定中存在的主要技术问题。 对是否考虑预期利润、如何考虑巨灾风险、是否考虑未来新业务等十个关键技术问题进行了深入讨论。
	7月16日	<ul style="list-style-type: none"> 开展了量化工作，过程中部分专家建议有以下建议： <ul style="list-style-type: none"> - 产品分类采用目前通用的14项分类； - 巨灾风险资本模型测试可由一家再保险公司负责； - 风险计量的时间区间可选用未来一年或到有效业务责任终止，最终结果可以根据不同的置信区间统筹考虑。
	12月	<ul style="list-style-type: none"> 完成了第一轮定量测试报告初稿，待提交偿二代领导小组办公室审议。

从以上的进度看来，各个项目组到年末都已经基本完成了风险量化的工作，并形成初步测试报告。但是，由于进一步风险量化的进展和整体框架设计必然有紧密的关系，因此业内人士更加关心整体框架的最终确定，这特别包括了是否容许采用内部模型、置信区间的标准，以及不同风险如何分类在不同的支柱中。

在欧盟偿付能力II的体系，以及巴塞尔II的银行资本监管体系中，金融企业可以选择使用统一的标准模型，或自行开发的内部模型。自行开发的内部模型对金融企业风险计量提出了更高的要求，但如能证明企业本身的资本要求低于标准模型的要求，将可以减少企业的资本投入。可是，监管机构如何认可内部模型，以及内部模型对外部投资者的低透明度，都是实施中的难题。

关于置信区间的设计，是指保险公司需要在一定的置信区间内拥有足够的资本应对相关的风险。譬如说现在欧盟偿付能力II设计的时间参数为1年，置信水平为99.5%，则表明保险公司有充足的资本抵御200年一遇的情景。置信水平越高，资本要求相应也需要提升。西方国家多采用时间参数为1年，置信水平为99.5%；但不少业内人士和投资者建议中国可以选择较低的置信水平，如95%。

此外，欧盟偿付能力II相对偿付能力I而言，除了风险计量精细化之外，增加了第二支柱风险评估和第三支柱披露的监管要求。此部分对于国内目前沿用偿付一代的保险公司而言是新的监管内容，对保险公司风险管理体系提出了更高的要求。目前，量化的资本监管和风险评估被视为两种割裂的监管要求，未来必然在统一框架下运作，这对保险公司和保监会都是新的尝试。

针对中国偿二代的改革，我们访问了北京大学金融数学系主任吴岚博士。吴博士担任了第三届保监会偿付能力监管标准委员会委员，并一直关注中国金融体系的资本监管建设。谈及中国偿付能力监管改革的难点，吴博士提出了两点：①虽然保险公司已经非常重视偿付能力，但偿付能力背后所揭示的资本与风险之间的关系并没有得到充分的理解。中国现行的偿付能力监管制度与风险之间的联系并不紧密，因此在改革当中需要提高对监管资本要求概念的进一步认识。②如果要建立与风险密切联系的资本要求，则必须建立一套服务于资本要求的风险评估量化体系，这就涉及对不同风险的量化手段，而这是精算师擅长并能够发挥作用的领域，中国的精算师应该更加关注如何提升中国的风评估技术水平。

偿付能力的改革将重大地改变资本约束的游戏规则。过去，以财产保险为例，如果原保费规模一致，不论是机动车险还是航天航空险，资本的要求是一致的，但这两种险种的风险存在很大的差异：前者是一种高频率、低赔付的业务，后者是低频率、高赔付的业务。在欧洲实施偿付能力II的过程中，产险公司发现短尾业务的资本要求有所减少，但长尾、波动较高的业务需要增加资本要求。中国的产险业务以短尾的机动车险为主，因此部分业内人士希望偿付能力改革能舒缓相关的资本要求。

我们认为在2012年，保险行业对偿二代改革的讨论还是不够充分。我们估计随着偿二代的研究工作在2013年不断展开，保险行业对偿付能力的改革会更加关注。

如何构建商业银行的数据分析能力

朱磊 合伙人
叶潇 经理
德勤上海事务所
企业风险管理服务

一、数据是银行的战略性资产

在银行业高度信息化的同时，盈利水平和发展规模也在不断扩大，积累的客户数据、交易记录、管理数据等呈爆炸性增长，海量数据席卷而来。信息未必一定通过数据来展现，但数据一定是信息的基础，海量数据意味着海量机遇和风险，可以通过多种方式为银行提供变革性的价值创造潜力。如何利用数据这一商业银行重要的资产来开展有效的分析和挖掘，从而促进管理并提升企业价值，是目前大多数商业银行所面临的重要挑战之一。

(一) 用数据帮助决策

目前国内银行业的战略发展和经营管理决策多数依赖于决策者的经验。面对激烈的市场竞争，管理层迫切需要数据的决策支持，提高经营和决策的科学性。银行各项产品能带来怎样的利润？如何判断客户是否有发展潜力？在哪里开设新的分行？将数据充分应用到经营管理决策的各个层面，这些原本看似很难做出回答的问题会变得清晰起来，管理者的决策过程实现由“依赖经验”逐步过渡至“有数可依”，在深入了解和把握银行自身乃至市场的状况的基础上，更加科学地评价经营业绩、评估业务风险、配置全行资源。

(二) 用数据提升管理精细度

随着银行业务转型及精细化管理的推进和深化，涉及资产、负债、客户、交易对手及业务过程中产生的各种数据资产，在风险控制、成本核算、资本管理、绩效考核等方面发挥着重要的作用。如银行贵宾卡服务，会考虑设置相应的资金要求和贵宾待遇，银行可以在分析本行客户数据的基础上确定最合适的目标客户群及期望达到的卡均余额和交易量。数据资产直接关系到业务管理的精细化水平，也是银行开展业务多元化、多方面分析的基础。“数据—信息—商业智能”将逐步成为商业银行定量化、精细化管理的发展路线，为有效提升服务能力提供强大支持。

(三) 用数据促创新、赢先机

我国商业银行提供的服务和产品存在较大的同质性，但比较竞争优势要求银行能够突破同质性，实施差异化战略。银行可以利用其掌握的数据资源，在客户挖掘、交叉营销、产品创新等方面大有作为，在零散的、无序的、历史的、当前的各种数据背后发现独特的业务规律，锁定特定客户群，根据不同市场需求和不同客户群制定相应的市场战略和产品服务方案，根据客户需求变化及时主动地开展业务及产品创新，在激烈的同业竞争中，通过充分利用数据取得先发优势，打造不可复制的核心竞争力。

(四) 用数据实现真正的全面风险管理

国际上，新《巴塞尔协议》对银行数据的广度、深度以及数据的完整性、准确性等方面提出了明确具体的要求，并将数据质量纳入操作风险的计量范围之内。在国内，各大监管机构也对银行提出了信息披露的要求，如资产负债表、利润表、统计报表、经营管理资料等。数据资产不仅是满足外部日趋严格的监管要求的客观需要，更是银行有效防范金融风险的必然要求，只有掌握全面的、权威的、合规的风险基础数据，才能准确地计算加权风险资产、构建风险模型、及时了解业务非正常变动、跟踪影响因子情况，从而更有效地防范金融风险。

在国内银行业加快转型发展的今天，如何评估最大化数据战略性资产的价值，已成为各家银行能否抢占先机、赢得优势地位的重要决定因素。

二、数据管理是实现数据资产价值的基石

目前国内银行普遍面临数据质量不高和数据支持决策的能力不强等问题，导致数据远未发挥其应有的价值。因此，数据问题已经成为银行提高竞争力的巨大障碍，主要表现在五个方面：数据管理职责不清、数据需求难以满足、数据标准不统一、数据质量不高、数据安全性不高。

为了有效解决数据问题，满足监管机构的要求，银行需要大力加强数据管理体系的建设，建立健全“目标方向、管理机制、执行规范”三层数据管理体系（见图1），着力解决业务、数据、技术三方面的分工与协作体系，为管理决策、业务经营、信息披露提供准确、快捷、全方位的信息服务，从而实现数据资产价值最大化，推动银行核心竞争力的持续提升。数据管理体系的实施过程应重点关注以下五大任务。

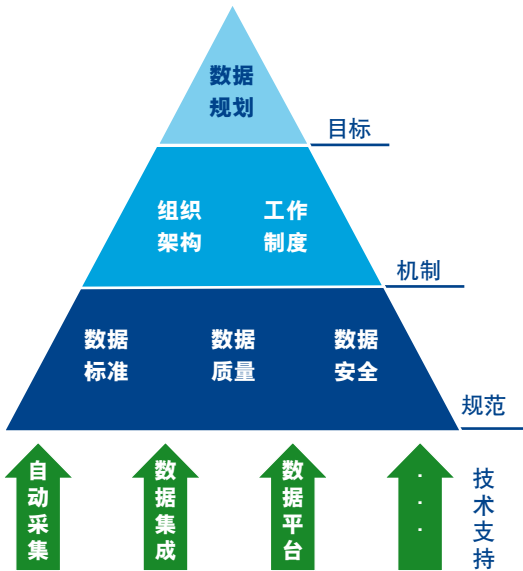


图1 数据管理体系框架

(一) 建立统一的数据规划目标

数据规划是数据管理体系的“指南针”。它根据业务对数据产生的需求，对满足业务应用的数据进行统一规划和协调管理，对现有数据和未来计划需求的数据进行前瞻性的管理工作，使数据能够适时地满足外部监管和信息披露以及内部经营管理、分析和发展目标的需求。数据规划的核心工作是针对数据生命周期的各个环节，提出相应的管理策略和原则，用以指导数据需求管理成果的落实。数据生命周期规划既需要针对数据应用制订方向性的策略，也需要为每个数据项指明相应的处理方法。

(二) 建立科学的数据管理工作机制

数据管理工作机制是数据管理体系的“基石”。数据管理工作机制的建设依赖于银行高层管理人员的重视和不断推动，同时也需要建立相应的数据管理机制的决策和控制机制。有效的数据管理需要明确专门的部门或组织承担整个银行的数据管理和应用职责。该组织负责从战略的角度进行统筹和规划，确定数据管理的范围，明确数据资产的归属、使用和管理等流程，明确数据管理的组织、功能、角色和职责，以及确定数据管理的工具、技术和平台等内容，切实有效促进数据共享、提高数据价值。

(三) 建立统一的数据标准规范

数据标准规范是数据管理体系的“粘合剂”。它是改进、保障和提高数据质量的依据，也是数据管理工作成败的关键。数据标准化是为了促成数据标准的形成和使用而进行的与之相关的一整套数据标准的规范，即制订和实施数据标准、提高数据管理水平过程。数据标准的制订需要参考行业监管和标准机构制订的数据标准，同时也应参考各个部门内部使用的特定数据的定义，制订出数据标准体系框架，可以分为基础类数据标准、业务类数据标准和应用类数据标准等，并在此标准基础上进行细分。在数据标准体系框架下，通过对数据标准的梳理工作，在业务属性和技术属性层面实现全行的数据标准化。

(四) 建立持续的数据质量管理规范

数据质量管理是数据管理体系的“助推器”。它是对支持业务需求的数据进行全面的质量管理，保障各项数据管理工作能够得到有效落实，达到数据准确、完整的目标，并能够提供有效的增值服务的重要基础。数据质量管理包括数据质量管理团队建设、数据质量管理制度建设、数据质量管理流程建设以及数据质量管理监控平台建设等。其中，数据质量管理监控平台建设至关重要。在数据统一管理的框架下，银行需要依据数据在生命周期各个阶段的特性，建立数据质量管理监控平台，及时发现数据质量问题，不断改善数据的使用质量，降低数据质量导致的业务风险，实现数据更大的应用价值，满足业务分析和管理决策的需要。2012年下半年，伴随上海银监局发起的“夯实统计信息基础，提升银行业数据质量”的竞赛活动，诸多银行从制度到流程启动数据质量的全面梳理核查。

(五) 建立完善的数据安全防范规范

数据安全防范是数据管理体系的“防护罩”。近年来，银行业有关数据泄露的事件时有发生，如何保障数据不被泄露和非法访问，已经成为数据安全非常迫切的问题。数据安全问题的解决，可以从以下五个角度着手：①制度及流程规范。通过建立数据安全和数据保密的相关管理制度和流程，合理划分数据安全级别，规范数据在生命周期中的安全。②数据安全意识。加强对数据所有者、数据管理者和数据使用者的安全意识培养，提高数据对于银行业务的重要性认识。③数据保密性。系统中的个人身份信息、银行账户信息等是否要进行加密，以避免数据被非法访问。④应用系统的访问控制。通过对应用系统的访问权限进行统一管理及单点登录，达到防止非法访问的目的。⑤数据安全审计。建立数据安全审计机制，检查数据中的安全风险，防患于未然。

三、数据分析是实现数据资产增值的重要手段

数据分析是指一整套技术、流程与应用工具，通过建立分析模型对数据进行核对、检查、复算、判断等操作，将样本数据的现实状态与理想状态进行比较，从而发现潜在的风险线索并搜集证据的过程。在实际应用中，数据分析可帮助银行作出判断，以便采取适当行动。因此，数据分析的过程就是组织有目的地收集数据、分析数据，最终使数据实现资产增值。

数据分析的目的是通过透视海量表面看似杂乱无章的数据，进行数据统计、定量分析、解释与模型预测，并通过基于事实的管理，找出隐藏在数据背后的内在规律和风险意义，最终推动整体决策。目前，数据分析在通信业、零售业和制造业等行业中已经得到广泛运用，而不少银行也已经于近几年开始着手建立用于业务经营分析的数据集市和数据仓库。

数据，作为银行重要的战略资产，在实现完善管理后，实施有效的数据分析是实现数据资产增值的最佳方式，也是唯一方式。

(一) 数据分析工作流程

一个基于风险导向的银行数据分析工作可以分为五个步骤进行，包括确定分析目标、基础数据收集、数据挖掘与分析、风险点跟踪以及数据指标固化。其中，数据挖掘与分析是整个工作流程中的核心关节。

1. 确定分析目标

明确的分析目标是确保数据分析过程有效的首要条件。执行分析的负责人需要明确具体的业务领域和相应的分析目标，并据此制订整体分析项目的进度计划、资源配置和结果评审等事项。

2. 基础数据收集

有目的地收集数据，是确保数据分析过程有效的基础。分析负责人需要对收集数据的内容、渠道、方法进行策划，根据分析目标确定需要获取的具体数据字段和数据结构，将识别的需求转化为具体的要求。

3. 数据挖掘与分析

完成基础数据收集工作后，便可以展开相应的分析工作。目前主要可以应用的数据分析方式有：数据质量复核、异常特征分析、探索性挖掘分析等。

4. 风险点跟踪

在通过分析得出结果后，需要对结果所揭示的问题进行进一步跟踪调查。这同样也是将数据分析结果与客观事实情况进行结合的过程，通过将空洞的数字指标落实为实际的业务问题行为来进一步拓展数据的价值。

5. 数据指标固化

最后对已经确认存在风险的数据特征进行系统固化，通过在数据集市或数据仓库中设置监控阈值，由信息系统对业务数据进行持续的指标性监控，以确保在第一时间发现新增类似风险事件，或者更进一步，将数据分析的结果作为持续审计或非现场审计平台的审计指标。

(二) 主要数据分析方法

目前银行业采用的比较典型的数据分析方法主要有：数据质量复核 (Data Quality Reconciliation)、异常特征分析 (Exceptional Analysis)、探索性数据挖掘 (Exploration Data Mining)。这三种数据分析方法对数据量和分析复杂度的要求也存在层级递进的关系。

1. 数据质量复核

复核分析即通过重计算和核对的方法对银行数据进行二次校验，以确保数据的完整性和准确性。主要包括：

- 存贷款利息重计算；
- 摊余成本计算复核；
- 票据贴现转贴现核算；
- 存贷款分户账与总账核对；
- 利息或息税调整时计息结息核算；
-

此类数据分析一般存在固定的分析计算方式，数据分析范围也以抽取样本的方式确定，对于分析工具的要求也可以根据需要进行计算的样本量选择电子表格或者小型数据库。从测试的本质上来说，此类数据分析更加接近计算机辅助审计技术的概念，是银行数据分析的基础类型。

2.异常特征分析

异常特征分析即根据数据中特定字段的相应特征，分析和筛选存在异常和风险的内容，并对结果进行进一步的跟进。分析对象主要包括：

- 违规处理的长期冻结账户；
- 异常计息息；
- 异常大额交易；
- 违规投资交易；
- 存贷款账户异常波动；
- ……

此类数据分析主要建立在确认存在风险的特定数据字段的基础上。数据分析范围一般根据测试期间的要求，选择一季度或一整年的全量业务数据；而数据分析工具则需要随着数据量增长的需要引入大型数据库来容载分析数据。

该类分析可以有效识别出银行业务流程中的潜在风险，而不仅仅局限于数据本身的准确性，是银行业数据分析的主要手段，同时也是非现场审计等自动化审计平台的核心审计模块。

3.探索性数据挖掘

探索性数据挖掘分析侧重于在数据之中发现新的特征，作为特征型数据分析的延伸，可以帮助分析者从看似无关的数据中挖掘出有意义的风险指标。

在这种分析中，除了数据本身，还需要引入成熟有效的数据分析模型，结合分析者自身的统计分析知识，综合运用，从而达到“发现数据背后的业务规律”这一目的。笔者在这里简要列示一些常用的数据分析模型，并给出模型适用的具体测试应用项目（见表1）。

此类数据分析主要依靠数学模型对数据本身进行规则归纳，并根据获得的规则进行风险判断。数据分析的范围除了测试期间的全量业务数据以外，还需要进一步获取前几个期间的数据作为数据建模元数据；而执行此类分析，所需要的工具除了数据库之外，还需要引入专业的统计分析工具进行数学建模。

表1 模型应用列举

功能	算法	典型应用
预测分析	决策树、贝叶斯网络、神经网络、主成分分析	贷款逾期预测分析、贷款人违约可能分析、欺诈探测
回归分析	线性回归、广义回归、Logistic回归	收益率预测，信用价值预测，客户潜在价值预测
聚类分析	K-平均值、多维尺度分析	支行风险对比、私人银行客户归类
时间序列分析	时间序列模型、神经网络	利率预测、投资损失预测、理财产品生命周期预测

通常的数据挖掘分析步骤为：获取历史违约数据并混合正常样本作为训练集；选择合适的数学模型进行数据挖掘，并生成预测规则；使用预测规则对目标测试数据进行分析；更新训练集对预测规则进行完善。

四、数据分析案例

笔者在此就以不良贷款预测分析和分支行业务健康度分析为例，简要阐述一下探索性数据分析的具体方法。

(一) 不良贷款预测分析

不良贷款率向来是银行的重要指标，如何降低不良贷款率，减少可能的贷款违约风险一直是银行管理层所关注的重点。通过有效的探索性数据挖掘，可以在对银行的历史违约贷款的数据特征进行归纳分析的基础上，得到有效的潜在违约贷款风险特征，从而对高违约风险贷款的发放采取更加严格的审批和复核。换言之，利用昨日的“失”，获取明天的“得”。具体的分析方式为：

- (1) 将历史违约贷款数据与正常贷款数据混合作为训练集，根据业务风险判断初步确定实还本息比率、贷款期限、贷款人信用评级、抵押物价值比率、担保方式等关键数据字段。
- (2) 选择合适的数学模型，比如C5.0决策树模型对训练集进行建模和规则归纳，根据信用审核职业判断以及模型置信度等指标，确定适合的数学模型和相应的特征阈值。

- (3) 使用模型对新增贷款项目进行验证, 判别高违约风险贷款。

(4) 最终形成树状判断结构。其中每一个节点都代表某个属性 (例如贷款企业的资产回报率小于某个特定值) 对该企业贷款违约可能性的影响和相应概率。
- (4) 最终形成有聚合倾向的点状分析结果 (见图 2)。图中每一个小方格均代表一个分支行实体, 并显著地聚合形成三类, 同时还存在若干无法明确地归于某一类的分行个例。

(二) 分支行业务健康度分析

对于规模庞大、分支行众多的商业银行来说, 如何有效监控和管理各个分支行是总行和高级管理层主要关注的重点。而通过数据分析中的聚类分析方法, 就可以有效地对各个分支行进行较为全面的横向对比, 从而了解各分支行的差异情况, 并根据结果量身定制发展方针。聚类分析的具体步骤如下:

- (1) 通过数据汇总和运算, 获取测试期间各个支行相应的指标数据, 包括存贷比、贷款损失率、综合收益率、综合存贷利率差。

(2) 选择合适的聚类算法进行聚类分析, 并生成聚类图表, 通过分析每个类群中代表性支行的特征, 来推断相应类群的特征。

(3) 对存在高风险的类群以及异常离群的分支行进行着重调查, 并通过数据分析统计结果, 明确对其聚类结果产生决定性影响的指标。

数据挖掘分析是银行业数据分析中的高级分析手段, 也是成熟完善的数据分析体系的标志, 即通过数据本身来分析数据, 形成企业数据增值的良性循环。

需要强调的是, 数据分析的方式并非相互孤立, 也并非线性地渐进演化, 而是应根据实际业务需求, 选择合适且有效的数据分析方法, 或结合和统一应用多种分析手段来达成目标。

随着对数据的管理从仅局限在信息系统层面, 扩展到整个银行的运营流程; 对数据的认识从单纯的信息转变为银行的重要资产; 数据的作用从支持业务运营的大后台, 走向确定管理决策的最前台, 笔者相信, 数据, 通过对其有效的管理与分析, 将会成为银行完善自身、实现增值的重要助推器。

注: 本文已发表于2013年2月的《银行家》杂志中, 但对其中内容进行了些许调整。

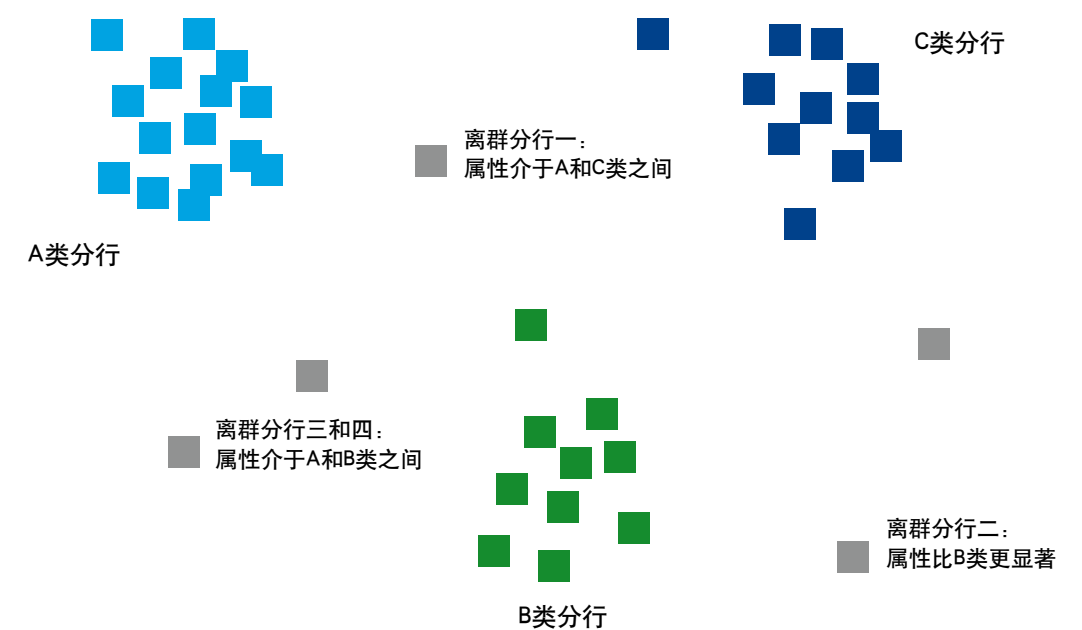


图2 聚类分析结果示例

低碳审计——浅谈内部控制评价与经济责任审计工作的整合

王 青 副总监
张晓茜 高级顾问
况成功 总监
德勤北京事务所
企业风险管理服务

现代社会倡导的“低碳经济”以节能降耗、提高能源利用效益为目标。与此概念相类似，作为内部监督要素的组成部分，内部控制评价、经济责任审计工作在技术方法上有共通之处，可以在审计标准、审计范围、审计程序、审计证据记录、问题发现等方面进行有机整合，避免重复工作，提高工作效率，从而实现异曲同工的目的。从某种意义讲，这样的整合过程也是一个“低碳化”过程。伴随着社会上出现如“低碳社会”、“低碳社区”、“低碳交通”等一系列蕴含低碳理念的词汇，我们将这种整合，称之为“低碳审计”。

一、相通的内部控制理论基础

内部控制评价和经济责任审计均运用系统化和规范化的审计流程和方法开展审计评价工作，尤其在内部控制方面存在共同点，为内部控制评价与经济责任审计的有效结合奠定了理论基础，也使整合具有可操作性。



内部控制评价		经济责任审计	
审计范围	<ul style="list-style-type: none">• 遵循重要性原则，以风险为导向	<ul style="list-style-type: none">• 遵循重要性原则，充分考虑审计风险；• 纳入审计范围的资产量一般不低于企业资产总额的70%，子企业数量不低于该企业总户数的50%	
审计内容	<ul style="list-style-type: none">• 围绕内部环境、风险评估、控制活动、信息与沟通、内部监督等要素进行评价；• 对内部控制设计与运行情况进行全面评价	<ul style="list-style-type: none">• 对内部控制建立及执行情况开展审计，审查企业内部控制的健全性、适当性和有效性；• 审查内容涉及内部环境、风险评估、控制活动、信息与沟通、内部监督	
审计标准	遵循《企业内部控制基本规范》、《企业内部控制应用指引》	可遵循或参照《企业内部控制基本规范》、《企业内部控制应用指引》	
审计方法	<ul style="list-style-type: none">• 个别访谈、调查问卷、专题讨论、穿行测试、实地查验、抽样和比较分析等多种方法；• 充分收集有效证据	<ul style="list-style-type: none">• 检查、观察、询问、重新计算、重新操作、外部调查等方法；• 获取充分、适当、可靠的审计证据	
工作底稿	记录企业执行评价工作的内容，包括评价要素、主要风险点、采取的控制措施、有关证据资料以及认定结果等	审计工作底稿包括：审计项目及审计事项名称；审计过程、审计结论及定性依据；索引号、所附审计证据的数量及清单；审计人员姓名、编制日期；复核人员姓名、复核意见、复核日期；被审计单位的意见、签字及盖章	

内部控制评价		经济责任审计
报告形式	对内部控制评价过程、内部控制缺陷认定及整改情况、内部控制有效性的结论等内容进行披露	主要包括审计基本情况、企业基本情况、被审干部的主要工作及成绩、审计发现、审计评价、审计意见和建议
审计结论	<ul style="list-style-type: none">（存在重大缺陷的情形）报告期内，公司在内部控制设计与运行方面存在尚未完成整改的重大缺陷（描述该缺陷的性质及其对实现相关控制目标的影响程度）。由于存在上述缺陷，可能会给公司未来的生产经营带来相关风险（描述该风险）；（不存在重大缺陷的情形）报告期内，公司对纳入评价范围的业务与事项均已建立了内部控制，并得以有效执行，达到了公司内部控制的目标，不存在重大缺陷	<p>根据所在企业内部控制的健全性、适当性和有效性情况，给予“××同志任职期间，制订和修订了××项管理制度，采取了××措施，内部控制有效（较为有效、无效）”的评价意见。</p> <ul style="list-style-type: none">“有效”的评价标准：内部控制健全、适当；内部控制执行有效，实现管理目标；“较为有效”的评价标准：内部控制较为健全；内部控制执行较为有效，基本实现管理目标，没有出现重大内部控制缺陷；“无效”的评价标准：内部控制不健全；内部控制执行无效，出现重大内部控制缺陷，没有实现管理目标
结果运用	内部控制评价结果和整改情况作为内部绩效考评的依据之一	作为对企业内管干部考核、任免、奖惩的重要依据

图1 内控评价与经济责任审计在内部控制评价方面的关系

二、整合思路浅析

有了整合的理论基础和可操作性，怎样整合才能充分发挥内部控制评价工作和经济责任审计的“整合”效应呢？

公司审计部门每年在安排经济责任审计和开展内部控制评价工作时，针对内部控制评价，可从以下几个方面对工作内容进行融合（见图2）。

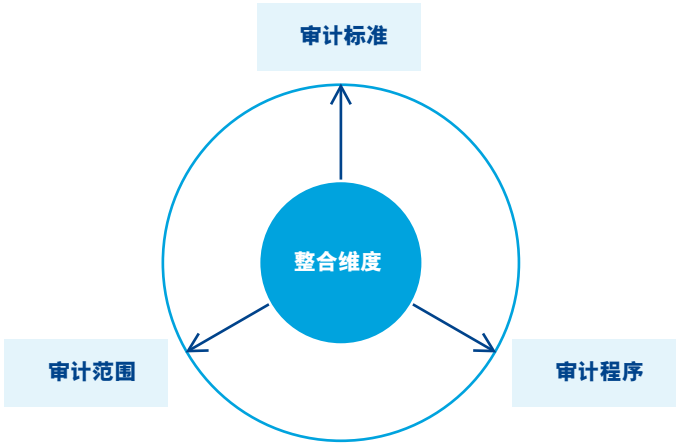


图2 内部控制评价和经济责任审计工作的整合

(一) 建立一致的审计标准

内部控制评价与经济责任审计对内部控制的评价基础是一致的，即围绕内部环境、风险评估、控制活动、信息与沟通、内部监督，对内部控制的健全性、适当性和有效性进行评价。

目前，很多企业已建立了较为完善的内部控制体系，明确了内部控制管理运行机制、内部控制标准等。通过这些内部控制标准，审视公司是否有相应的制度设计以满足内部控制要求，以及制度是否执行到位。因此，就内部控制而言，无论是内部控制评价还是经济责任审计，都可将内部控制标准作为内部控制审计评价的依据。

(二) 确定共同的审计范围

结合内部控制评价范围确定原则及《内部审计实务指南第5号——企业内部经济责任审计指南》中关于审计范围确定的相关规定，两者在确定审计范围时，都需要遵循重要性原则，以风险为导向，确定重要性水平，以及重要企业和重要业务流程。因此，公司可从财务报表角度入手，通过定量和定性的角度，考虑对内部控制、财务报表以及审计工作可能产生影响的多种因素，确定重要子企业和重要业务流程。

(三) 形成统一的审计程序

如同地图对旅行者，审计程序是指导具体审计评价工作的重要工具。俗话说“工欲善其事，必先利其器”，在确定了一致的审计标准和审计范围后，如何进行审计程序的融合，成为推动内部控制评价与经济责任审计工作有效整合的关键环节。

1. 审计程序的融合

进行融合时，以某一程序为基准，如以经济责任审计程序为基准，将内部控制评价测试步骤与其进行匹配，发现需要补充和细化的程序，从而形成统一的审计程序，实现一套工作底稿满足两种工作需要。

2. 样本量的选择

在实施审计程序的过程中，针对每个控制检查点，需要抽取多少个样本，才能既支持测试的结论，又可以在一定程度上减少工作量。样本量的选取是不是多多益善呢？公司可以考虑对审计程序所对应的检查点进行等级分类，明确不同等级的检查点的抽样规则，以提高审计工

作的效率。在确定检查点等级时，可通过是否与财务报表认定相关、风险评估结果、发生过的风险事件、业务性质、历史事件、以往审计发现等综合确定。例如，根据是否与财务报表认定相关（直接/间接/非相关）、风险评估结果对检查点进行等级分类，可划分为4档，进而确定不同等级下所选取的样本量（见表1）。

表1 根据是否与财务报表认定相关、风险评估结果进行检查点等级分类

	检查点风险评估结果		
	高	中	低
财务报表认定直接相关	1档	2档	3档
财务报表认定间接相关	2档	3档	4档
财务报表认定非相关	3档	4档	不执行测试

3. 审计期间的考虑

虽然内部控制评价工作和经济责任审计根据上述内容在审计标准、范围以及程序上可以有效整合，但在整合过程中仍需要对检查期间进行分析，以确定是否需要补充额外工作。

通常，内控评价期间为评价当年，而经济责任审计期间会结合审计目的而有所不同。例如，对领导的离任审计期间为其任职期间，该任职期间可能是内控评价年度以前，也可能是任职到内控评价年度中的某一段时间段。如何在审计期间不一致的情况下，保证整合测试的有效性呢？在审计期间完全不同或是部分重合的情况下，即经济责任审计涉及的内控评价当年以前的审计期间，可根据经济责任审计需要，参照内控评价当年选取样本量，酌情减少经济责任审计其他期间的样本量，从而提高审计效率。

三、结束语

将内部控制评价与经济责任审计工作进行有机整合，实现“低碳审计”，是值得进一步研究和探讨的。伴随着内部控制评价与经济责任审计整合工作的初步尝试和不断实践，这种整合方式将被逐步运用到其他管理工作中，如专业部门的专项检查、与风险管理工作的结合等，从而真正实现内控工作与其他管理工作逐步紧密结合，发挥联动效益。

保险业风险管理小故事 (5)

谁审批了那笔交易？

施建俊 副总监

德勤上海事务所
企业风险管理服务

描述

李秘书：“王总，上次我和你说的那个申请你看怎么样啊？”

王经理：“没什么问题，我这几天在出差，没法登录系统，等回来我就审批。”

李秘书：“可是王总，我现在急着要啊，这次的交易很大，领导们都很重视，要是因为审批太晚让这件事情黄了，我和你都担不起这个责任啊！”

王经理：“这样吧，你用我的用户名进系统批一下吧，我的用户名是*****，密码是*****。”

几天后

张经理：“老王啊，上周你批的两笔交易里有一笔可是会议上明确说不能批的啊！怎么回事？”

王经理：“上个礼拜我在外面出差，都没上网，怎么审批？哦，对了！我让李秘书帮我批了一笔，可是……（汗）？”

王经理：“小宋，能查出上周我在系统内的操作日志吗？”

小宋（系统管理员）：“好的，王经理，我看一下系统日志，您上周登录了两次系统，时间分别是……”

王经理：“果然我的账号被盗用了啊！”

分析

信息系统控制是《保险公司内部控制基本准则》运营控制中不可或缺的控制环节。信息系统控制一般分为整体控制和应用控制。整体控制是指对企业信息系统开发、运行和维护的控制；应用控制是指利用信息系统对业务处理实施的控制。

上述案例揭示了信息系统控制中整体控制上的缺陷。通俗地说，信息系统整体控制是信息系统部门日常所进行的一般业务管理，它是衡量信息系统整体是否可信赖的机制。对于用户账号和密码共享，系统日志无法辨别登录者的真实身份。如果必须共享账号，那么须明确定义共享目的和共享账号的权限，并由管理层进行确认。此外，用户账号、权限管理和密码设定作为信息安全领域要求中最重要的内部控制，在使用情况发生改变后，应及时更换密码，对用户账号和访问权限进行相应的赋予、变更或删除。也就是说，王经理在授权李秘书审批交易后，应该及时修改自己的密码，保证账号的安全。即使在平时，也应设定安全系数较高的密码，妥善保管并定期变更。

内控小字典

用户账号管理的基本要求

企业应当建立用户管理制度，加强对重要业务系统的访问权限管理，定期审阅系统账号，避免授权不当或存在非授权账号，禁止不相容职务用户账号的交叉操作。

企业应当在信息系统中设置操作日志功能，确保操作的可审计性。

公司应按照“谁主管、谁负责，谁运营、谁负责，谁使用、谁负责”的原则，明确信息安全各相关方的责任，加强人员管理，强化信息安全意识，全面落实信息安全管理责任制。

注：本文参照《企业内部控制应用指引第18号——信息系统》和《保险公司信息化工作管理指引（试行）》相关内容。已发表于《太平洋保险报》2011年4月1日，总第649期。

企业内部控制实务 (9)

——资金管理

与资金有关的舞弊将动摇企业的根基

原国太郎 合伙人

德勤上海事务所
企业风险管理服务

金融衍生产品管理：

企业需要的是明确的、具有可操作性的政策

与资金有关的交易产品中，一般认为风险最大的应该是金融衍生工具。实际上，“衍生工具”这个词本身就会给人感觉是偏离实业的金融机构的产品。但是，衍生工具原本是一方支付一定的手续费从而降低风险，另一方收取手续费以承担风险的交易，是如同保险一样，自然产生的产品。

实际上，世界上最初使用现代衍生产品的是日本江户时代1730年开设的位于大阪堂岛米会所的期货产品。诸藩有实际需求，希望确定预备生产的大米的价格，并将一部分变卖。米商接受未来商品价格，并可以对权利凭证本身进行交易以赚取净利润。

让我们再向前追溯，如果列举人类最伟大的30项发明，货币一定会名列其中吧。世界各地根据实际需要，自然而然地产生了各种材质、各种形状的货币。随着产业的发展和经济活动的复杂化，交易方式当然也越来越进步。

但是工具和技术若使用不当，将带来危险。比如火和刀都是非常便利的人类发明，但是同时要注意不能被烧伤或者刺伤。同样道理，在使用衍生产品的时候也要建立适当的风险管理手段（内部控制）。

关于衍生工具的内部控制，首先要注意的是建立使用衍生工具的明确制度。到底是根据实际需要（风险对冲）来使用衍生工具，还是出于追逐利益的原因使用衍生工具（投机）？一般来说，除了业务本身即是承担投资风险的金融机构和投资基金，其他的企业应该在公司内部规章中说明衍生工具必须仅为风险对冲而使用，并进一步限定使用种类，例如，仅限于汇率远期、利率掉期等具体的工具。

即使是根据实际风险对冲需要使用衍生工具，管理层的审批仍然必不可少。如果与投机活动相关，企业必须根据实际承担风险的程度建立相应的审批手续和规则。

可以参考套期会计的原则来判断使用衍生工具的目的

然而，人们往往难以判断是不是真的根据实际风险对冲需要使用衍生工具。比如，企业预测到会有外币计价的订单，于是不得不进行相应的采购和生产活动，为了锁定利润额，自然会尽早约定远期汇率。但是，从理论上讲，在订单还没有确定的情况下就约定汇率，相当于将全部利润暴露于汇率风险下。

套期会计相关的会计准则可以成为一个判断标准。因为企业可以考虑不同的衍生工具是否适用套期会计，它们在财务报表及附注中有不同的披露要求。但是，套期会计相关的会计准则在美国、日本和中国（套期会计和国际财务报告准则非常相近）这三国之间目前来说都有很大的不同。

对于已经使用的衍生工具，企业必须建立良好的台账管理，记录合同的条件、金额、风险说明及衍生工具的对方。

而且，尤其重要的是，企业须确认衍生工具合同实际上和交易对手互相核对。具体举例来说，由和衍生交易无关的独立的其他交易人员从交易对手处获取计算表，并与公司内部的衍生工具台账相对照。

中国航油（新加坡）股份有限公司（简称“中航油”）是一个典型的衍生工具投机失败的案例。经国家有关部门批准，中航油自2003年开始做油品套期保值业务。但管理层擅自扩大业务范围，从事石油衍生品期权交易，但一直未向中国航油集团公司报告，中国航油集团公司也没有发现。该期权交易致使中航油在清算时造成账面实际损失和潜在损失总计约5.54亿美元。2005年6月3日，外部会计师发布了有关中航油巨额亏损的最终调查报告。报告认为若干因素单独或共同造成了公司在期权投机交易上受到损失，包括没有按照行业标准对期权仓位进行估值；没有正确地在公司的财务报表上记录期权组合的价值；缺乏针对期权交易的适当及严格的风险管理规定；公司管理层有意违反本应该遵守的风险管理规定等。

另一个典型案例是中国国储局2005年的铜期货巨额亏损事件。中国国储局一名交易员在LME（伦敦金属交易所）铜期货市场上通过伦敦金属交易所场内会员SEMPRA，在每吨3000多美元的价位附近抛空，建立空头头寸约15万~20万吨。铜价格的一路上涨给国储局带来巨额损失。另外，在国储铜事件上，交易行为由原来的两个岗位变成由该交易员一个人操控，背离了内部控制职务分离的原则。

衍生工具的市值确认非常重要。企业须对衍生工具的财务特点进行充分了解和评价，并由管理层建立相应的制度。

在中国，似乎使用金融衍生工具的企业为数尚少。但是，还是有些公司使用了衍生工具，以此减少了原材料价格高涨对经营的影响，并实现了比同行更高的利润。如开头所述，企业通

过衍生工具的使用，可以降低风险。企业须以构筑完善的管理体制为前提，积极地审视衍生工具的管理。

**投资、借出资金的管理：
企业应以发展主营业务为重**

无论是投资还是借出资金，企业都须根据金额和风险程度确定相应的管理层审批权限。而且和衍生工具相似，投资和借出资金也必须实施台账管理并定期通过市值评估。

由于投资和借出资金记为资产，所以内部控制方面必须确认其真实存在性。资产的确认必须由不负责该资产管理的其他人员实施，这一点尤为重要。

上市公司浙大海纳2003年年报、2004年半年报披露的银行存款都有两亿多元，但在这期间，大股东及关联方多次私自从公司账户上划走巨额存款，实际银行存款不到一半。另外，大股东不仅喜欢现金，还喜欢国债。截至2004年半年报，披露的债券投资额实际上全部落入了关联方的囊中，公司的国债账户空空如也。大股东有此“胃口”，上市公司也在行动上予以配合。

此外，投资或借出资金对象无论是谁，都不像衍生工具那样简单地是一个承担风险或是降低风险的问题。这关系到留存资金的运用、采购方和销售方的支持、和同行业企业的合作、对子公司和关联方的出资等考虑，还和本业相关的各种战略目标都相联系，并不是单纯的承担风险。

近年来，面向消费者生产商品的制造业也开始顺利地开展金融业务。通用电气、通用汽车的财务公司特别有名。它们从方便消费者购买自己公司产品的金融贷款起步，通过赊销收取利息，帮助了主营业务的发展。

面向消费者的金融，其本身有很高的利润率。但是如通用汽车，主营业务虽然不景气，但是财务公司业绩很好，这恐怕只是数字的游戏。在美国，相关的融资和信用卡使用已经非常普遍。在这样的地方，制造商的价格战略中，首先考虑的是降低利率，其次才是商品本身的降价。通用汽

车的“零利率”策略在媒体上也有报道，这样低的利率只是为了促进消费者购买产品而已。

在会计处理上，对于财务公司来说，因为利息收入是“营业收入”，财务公司根据消费者的信用状况将正常的利息记为营业收入，而与实际利息的差额部分由汽车公司通过销售费用对财务公司予以填补。在财务报表的分部报告中，看起来好像主营业务不景气但是财务公司业绩很好，实际上利息的减免是产品打折促销的一种手段，我们应该将主营业务和财务公司业务合并起来分析财务报表。

**借入资金的管理：
还款到期日检查和资金周转**

借入资金有多种形式，除了简单地从金融机构借入资金，还有公司债券、可转换公司债券以及资产支持证券等形式。资产支持证券是以资产为担保借入资金的形式。它不仅是资金周转的问题，而且是以应收账款为资产对象，在财务报表上多表现为出售应收账款以回笼资金。资产支持证券在2006年5月16日中国证监会发布的《关于证券投资基金投资资产支持证券有关事项的通知》中已经提及，但是实际使用的很少。

借入资金的内部控制，从基本要素上说，就是和存在性相关的审批、台账管理以及和交易对手的复核（具体来说，就是从贷款人处获得计算表并和台账相对照）。如果从借入资金本身的特点来看，到期还款日检查和相应的资金周转管理显得非常必要。

对于附有财务限制条款（Covenant Clause，比如合同规定，股本比率、分红情况等财务数值须确保在一定数值以上或者以下）的借入资金，为了遵守财务限制条款，企业必须有定期的复核。公司债券发行附条款的情况往往比较多。即使是从金融机构借入资金，在金额巨大或者内容复杂的情况下，例如，针对公司所有的应收账款进行资产支持证券化时，金融机构有时候会要求公司维持某些财务指标在一定值以上。

与财务相关的三个方面的审查要点

表1总结了与财务相关的三个主要方面的内部控制审查要点。

表1 和企业相关的环境要素相互关系

	审批	台账管理	检查点风险评估结果			
			市值评估	对交易对手的确认	资金周转	财务限制条款
衍生工具	○	○	○	○		
投资、借出资金	○	○	○	○		
借入资金	○	○		○	○	○

关于台账管理，固定资产的台账往往通过简易的软件或者表格计算管理，必须关注安全和备份等信息系统整体控制。同样，这也适用于衍生工具、投资、借出资金和借入资金的台账管理。特别是借入资金的还款和衍生工具的履行，若操作上有差错，将带来严重的后果。

关于借出资金和借入资金，包括现金管理、现金流量系统控制在内的全面管理可能是最佳实践。对于衍生工具，虽然系统并不适合于管理特殊和复杂的事物，但是根据实际需要不得不采用衍生工具交易的情况下，由于汇率远期约定等已是定型的工具，根据交易规模和数量，还是由系统管理比较合适。

由于公司债券被记入负债类会计科目，企业需要实施与借入资金相关的内部控制。除此之外，由于公司债券属于公开发行的有价证券，对于其发行、偿还需要实施和股票相同的管理。至于可转换公司债，需要做潜在性稀释股票（Dilutive Security）计算，其商业上的性质和管理渐渐接近股票。

出资方作为股东影响公司的经营是理所当然的。然而，如前所述，如借款金额巨大，那么公司的经营状况和借出资金者也会存在重大的利害关系。很早之前，财务报表的最初目的就是为债权人提供财务信息。

所有者权益的管理：

今后的课题是，怎样的“内部控制”适合企业

所有者权益从本质上来说，不会发生经常性的交易。迄今为止，还很少有人考虑所有者权益需要怎样的内部控制。可以想到的内部控制包括（包括股本变化的）资本明细的定期复核、与登记簿和从证券代理机构（信托银行）获得的股东名单相互对照。

股票的发行、减资等与《公司法》、《证券法》等多个法规制度相关。为了准备好董事会决议、对股东和债权人的通知、登记等合规性要件，企业必须准备一份检查用的一览表（可以从证券代理机构等处获得），在股本变化的实施过程中使用。同样道理，公司债券、可转换公司债券也以此为准。

中国的上市公司屡次出现虚假出资、挪用资金等事件。比如20世纪90年代曾被称为“中国股市第一案”的“红光案”，红光实业涉嫌虚假出资，编造虚假利润，骗取上市资格；少报亏损，欺骗投资者；隐瞒重大事项，挪用募集资金违规买卖股票，未履行重大事项的披露义务。骗取配股资金也是上市公司的重大舞弊手段之一。比如山东巨力公司原董事长和原财务处副处长涉嫌虚增1999年年度利润16145.73万元，骗取了配股资格，于2001年在深交所配股发行股票1149万股，共募集资金15971.1万元。公司成功配股之后，多项配股募项目却发生变更。相关负责人由于涉嫌欺诈发行股票被追究刑事责任。

也许人们认为内部控制（尤其是在传统的业务流程层面上的内部控制）难以防止上述舞弊事件的发生。然而，今天的内部控制登上历史舞台的契机是，安然和世界通讯通过虚假报告以哄抬股价的舞弊事件。由此，2002年美国制定了企业改革法——萨班斯（SOX）法案。

尝试对“股份公司”体制作出新调整

中国于1990年成立了上海证券交易所和深圳证券交易所，普通市民可以通过交易所进行证券交易。证券交易所的成立为中国经济发展奠定了良好的基础。

实际上，“股份公司”和“货币”一样，被称为人类的伟大发明之一。股票市场是一个中介场所，连接了拥有生意和业务但是没有资金的人，和虽然有资金但是不能有效使用的人。它使得社会整体资金利用的有效性取得了飞跃性的提高。股份公司这种组织方式的广泛采用，也支持了产业革命。

人们从早期开始就对“资本主义”的各种缺点提出批判。自由竞争的结果，是胜者垄断或者成为寡头，从而变得缺乏效率。

所有的体制都需要管理维护和调整。在现代经济中，股份公司高速发展和日趋复杂。“内部控制”的明确义务也许是股份公司尝试的调整之一，包括美国SOX法、日本版SOX，还有中国的《企业内部控制基本规范》及其指引的征求意见稿等都是对其的最新锐尝试。

注：本文已发表于《中美日企业内部控制实务》一书中，但对其中内容进行了些许调整。

德勤中国企业风险管理服务的联系方式

北京

德勤华永会计师事务所（特殊普通合伙）
北京分所
北京市东长安街1号
东方广场东方经贸城德勤大楼8层
邮政编码: 100738
电话: +86 10 8520 7788
传真: +86 10 8518 1218

上海

德勤华永会计师事务所（特殊普通合伙）
上海市延安东路222号
外滩中心30楼
邮政编码: 200002
电话: +86 21 6141 8888
传真: +86 21 6335 0003

台湾

勤业众信联合会计师事务所
台北市民生东路三段156号12楼
邮政编码: 10596
电话: +886 2 2545 9988
传真: +886 2 2545 9966

香港

德勤·关黄陈方会计师行
香港金钟道88号
太古广场一期35楼
电话: +852 2852 1600
传真: +852 2541 1911

深圳

德勤华永会计师事务所（特殊普通合伙）
深圳分所
深圳市深南东路5001号
华润大厦13楼
邮政编码: 518010
电话: +86 755 8246 3255
传真: +86 755 8246 3186

广州

德勤华永会计师事务所（特殊普通合伙）
广州分所
广州市天河路208号
粤海天河城大厦26楼
邮政编码: 510620
电话: + 86 20 8396 9228
传真: + 86 20 3888 0119 / 0121

德勤中国公司治理中心网址: www.corpgov.deloitte.cn

德勤中国公司治理中心（本“中心”）于2010年4月21日正式宣告成立。中心将作为中国公司治理实务发展情况的信息集散地，并面向中国境内各位董事、高管与投资者主办各类重大公司治理活动与圆桌会议。中心的建立旨在促进中国内地和香港特别行政区两地的公司治理的领先实践。它着重介绍了在中国内地和香港特别行政区两地处于领先地位的公司治理实践，并重点收集来自德勤中国和其他第三方的多元化的关于公司治理的资源及领先理念。

《德勤企业风险》(第六辑) 读者调查问卷



1 针对以下方面, 请您评价《德勤企业风险》(每项单选):

请您按照以下标准打分:	5(非常好)	4(较好)	3(说不准)	2(较差)	1(非常差)
内容	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
图片	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
版式	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
编读互动	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2 《德勤企业风险》(第六辑) 的文章是否对您有所帮助(每项单选):

请您按照以下标准打分:	5(很有帮助)	4(有些帮助)	3(说不准)	2(没什么帮助)	1(没有帮助)
如何通过数据丢失防护系统(DLP)应对日益严格的信息保护法规及监管要求?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
个人信息保护立法及监管要求	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
个人资料保护制度建置项目经验谈	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
个人信息保护趋势浅谈	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
企业因应个人资料保护的建议	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
隐私保护的企业现状和合规挑战	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
管理数据隐私的利器——身份和访问管理	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
个人资料泄漏调查经验分享	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
企业敏感信息保护之道	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
银行信息科技安全风险管理探讨	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
当前宏观背景下租赁行业的机遇、风险和创新	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2013年中国保险业十大趋势与展望(上)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
如何构建商业银行的数据分析能力	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
低碳审计	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
保险业风险管理小故事(5)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
企业内部控制实务(9)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3 您最想了解关于风险管理和企业内部控制的相关内容(可多选)

- | | | | | |
|-----------------------------------|---|-----------------------------------|----------------------------------|--------------------------------|
| <input type="checkbox"/> 全面风险智能服务 | <input type="checkbox"/> 资本市场服务 | <input type="checkbox"/> 合规性准备及协助 | <input type="checkbox"/> 业务持续性规划 | <input type="checkbox"/> 信息治理 |
| <input type="checkbox"/> ERP控制 | <input type="checkbox"/> 安全电子商务 | <input type="checkbox"/> 内部审计 | <input type="checkbox"/> 合同风险与履约 | <input type="checkbox"/> 计算机审计 |
| <input type="checkbox"/> IT尽职调查 | <input type="checkbox"/> 其他: 请具体描述您感兴趣的相关内容 | | | |

4 您今后是否想继续收到德勤中国提供的《德勤企业风险》以及宣传资料? (☐ 是 ☐ 否)

烦请您提供贵公司以下信息, 我们将会把贵公司的资料注册在发送名单中。

公司名称: _____

联系地址: _____

联系人姓名: _____

联系电话: _____

联系人电子邮箱: _____

5 您是否觉得阅读电子版《德勤企业风险》杂志更为便捷?(每项单选):

请您按照以下标准打分:	5(非常同意)	4(较同意)	3(说不准)	2(不太同意)	1(不同意)
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

您填写完成读者调查之后, 可以发送传真或电子邮件到以下联系方式:

+86 21 6335 0003 企业风险管理服务《德勤企业风险》编委会 收

您填写完成读者调查之后, 也可以通过邮寄到以下联系地址:

中国上海市延安东路222号外滩中心30楼 邮政编码200002

德勤华永会计师事务所(特殊普通合伙) 企业风险管理服务《德勤企业风险》编委会 收

感谢您的阅读与合作!

巍巍交大 百年书香
www.jiaodapress.com.cn
bookinfo@sjtu.edu.cn



责任编辑 / 吴咏蓓
封面设计 / 顾弘敏
责任营销 / 陈大凯

关于德勤全球

Deloitte (“德勤”) 泛指德勤有限公司(一家根据英国法律组成的私人担保有限公司, 以下称 “德勤有限公司”), 以及其一家或多家成员所。每一个成员所均为具有独立法律地位的法律实体。请参阅 www.deloitte.com/cn/about 中有关德勤有限公司及其成员所法律结构的详细描述。

德勤为各行各业的上市及非上市客户提供审计、税务、企业管理咨询及财务咨询服务。德勤成员所网络遍及全球逾150个国家, 凭借其世界一流和高质量专业服务, 为客户提供应对最复杂业务挑战所需的深入见解。德勤拥有约200,000名专业人士致力于追求卓越, 树立典范。

关于德勤大中华

作为其中一所具领导地位的专业服务事务所, 我们在大中华设有21个办事处分布于北京、香港、上海、台北、重庆、大连、广州、杭州、哈尔滨、新竹、济南、高雄、澳门、南京、深圳、苏州、台中、台南、天津、武汉和厦门。我们拥有近13,500名员工, 按照当地适用法规以协作方式服务客户。

关于德勤中国

在中国大陆、香港和澳门, 我们通过德勤 关黄陈方会计师行和其关联机构包括德勤华永会计师事务所(特殊普通合伙), 以及它们下属机构和关联机构提供服务。德勤 关黄陈方会计师行为德勤有限公司的成员所。

早在1917年, 我们于上海成立了办事处。我们以全球网络为支持, 为国内企业、跨国公司以及高成长的企业提供全面的审计、税务、企业管理咨询和财务咨询服务。

我们在中国拥有丰富的经验, 并一直为中国会计准则、税制以及本土专业会计师的发展作出重大的贡献。在香港, 我们为大约三分之一在香港联合交易所上市的公司提供服务。

本文件中所含数据乃一般性信息, 故此, 并不构成任何德勤有限公司、其成员所或相关机构(统称为“德勤网络”)提供任何专业建议或服务。在做出任何可能影响自身财务或业务的决策或采取任何相关行动前, 请咨询合资格的专业顾问。任何德勤网络内的机构不对任何方因使用本文件而导致的任何损失承担责任。

上架建议: 企业管理

ISBN 978-7-313-09784-2



9 787313 097842 >

定价: 30.00元