企业风险

企业风险管理服务
季刊
第3期
2011.03

特集 信息技术风险－思考当代企业不可或缺的基础设施建设

访谈 台湾土地银行信息风险管理经验交流

2010全球安全调研报告

企业安保：介绍企业安保风险抵御系统（增强版）

管控IT风险，提升IT价值

加强电子银行交易风险管理，提升客户安全体验

Web应用安全，您再也无法忽视的风险

双管齐下 高枕无忧－数据防泄露在行业中的应用

新环境下的企业信息系统日志分析

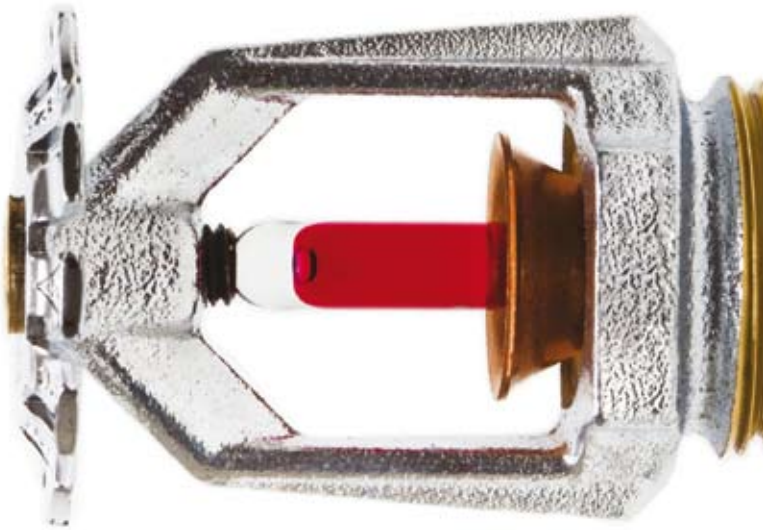
自动化风险管理

研究室 财金咨询－ITIL信息服务管理最佳实务

连载 企业内部控制实务（3）－销售流程（2）收入确认、催款、收款

推荐书籍 赢（Winning）第四版

企业风险用语 业务持续性管理（Business Continuity Management）



Deloitte.
德勤

2011年3月，第3期
企业风险
德勤中国，企业风险管理服务出版

企业风险出版委员会
刘伟杰
廖福良
薛梓源
黄皓礼
陈嘉祥
林允纲
方烨
谈亮
蒋黎虹

编制
原国太郎
孙永杰
冯芷翠
戴忆婷
赵理
金睿
何萍
庄宇杰



编者的话：

首先感谢各位关注本期的企业风险杂志。本期刊物出台之时，春回大地，万物复苏，回顾过往一年中与诸多公司管理层在风险管理领域的专业探讨，本人欣喜地发现，受益于信息技术的广泛应用，各行各业的客户已经越来越多地关注到信息技术领域的风险并在采取积极的措施进行应对，因此，本期杂志将以“IT风险”为主题，集中讨论企业如何管理和应对与信息技术有关的风险。

众所周知，IT与业务的融合，在给企业带来效率提升，协助企业打造可持续发展的核心竞争力的同时，也加剧了业务可能面临的风险。由于信息系统失效所导致的业务中断事件已经屡见不鲜，因此，任何注重IT与业务融合的企业，都应该像管理其他业务风险一样管理IT风险。事实上，IT风险也已经成为领先的风险智能企业实行全面风险管理的重要内容。从范围上看，IT管理和应用的各个领域诸如IT治理、信息安全、系统开发、系统运维、外包、业务连续性等方面的管控措施不到位都可能导致IT风险事件的发生，因此，本期杂志在内容组织上，既包括了介绍全球信息安全和IT风险趋势的调研报告，也包括了诸如Web应用安全、安全日志分析、安全风险管理等技术领域的探讨，此外，我们还从业务发展的角度，与各位分享对深度依赖IT的业务风险进行管理的解决方案，包括电子银行交易风险以及研发信息资料的安全保护等。

除了企业自身的风险管理需求，国家以及行业方面的监管机构也纷纷出台了涉及信息技术风险管理的监管要求，例如国资委的《中央企业全面风险管理指引》、银监会的《商业银行信息科技风险管理指引》等等。我在与监管机构以及公司的高层沟通时，经常会就如何兼顾多个监管机构要求，如何将IT风险与企业风险管理深入融合，如何构建有效的信息科技风险管理机制，如何实现IT风险管理工作的常规化、日常化等有关话题进行深入探讨，这些管理层所提出的问题都一针见血，直接指出了实现有效IT风险管理的关键所在，而针对这些问题的解决方案也是我们成功实施IT风险项目的重要因素。

IT风险管理既是一个新的话题，又是一个老的话题，“新”是因为我们在逐步从风险管理的角度上审视IT管理不当对业务所造成的潜在威胁和影响，“老”则是因为我们其实一直所从事的IT管理工作实质上也都是为了规避风险，实现业务价值的最大化。做为一家在风险管理领域，尤其是在IT风险管理方面多年位居行业领导地位的专业服务机构，我们衷心希望本期刊物中的观点与见解对您有所启发，帮助您开拓IT风险管理的工作思路，我本人也非常期望能与我的同事一起与您深入探讨IT风险的专业问题。

薛梓源
德勤北京事务所
企业风险管理服务
合伙人

目录






特集 信息系统风险－思考当代企业不可或缺的基础设施建设

访谈

2 咨询风险管理大跃进–台湾土地银行信息风险管理经验交流

4 2010全球安全调研报告

17 企业安保：介绍企业安保风险抵御系统（增强版）

19 管控IT风险，提升IT价值

25 加强电子银行交易风险管理，提升客户安全体验

30 Web应用安全，您再也无法忽视的风险

32 双管齐下 高枕无忧－数据防泄露在行业中的应用

37 新环境下的企业信息系统日志分析

41 自动化风险管理

研究室

46 财金咨询－ITIL信息服务管理最佳实务

连载

51 企业内部控制实务（3）–销售流程（2）收入确认、催款、收款

企业风险用语

56 业务持续性管理（Business Continuity Management）

推荐书籍

58 赢（Winning）第四版

Always one step ahead!
信息风险管理大跃进
– 台湾土地银行信息风险管理经验交流

吴佳翰 合伙人
温绍群 经理
黄永婷 经理
德勤台北事务所
企业风险管理服务

受金融海啸影响，国际经济环境与金融市场整体情势历经低潮，造成市场不稳定的因素日益增加，加上各种类型银行激烈竞争，面对银行业务多元化经营与全球化竞争，银行的经营环境日益复杂且潜在风险水平逐渐提高。本文透过专访台湾土地银行信息处陈怡宏处长，了解台湾土地银行信息处所面临的信息风险与挑战，并从信息的角度谈如何控制任何引起损失或降低获取利润的因素，使企业达成既定的目标。

台湾土地银行(以下简称「土银」)为台湾公营行库之一，是台湾唯一办理不动产信用的专业银行，除贯彻推动住宅、土地政策，发展国民经济建设等专业银行使命外，更以「创新、效率」企业化经营方式，运用不动产专业利基，深化业务基础，积极转型为企业提供金融服务、土建融并进，个人和企业业务共同发展的全方位服务银行，并朝亚太地区区域性优质金融机构的愿景迈进。

土银面对的信息风险管理重点与挑战为何?

身为公股银行，土银担任民营银行的模范生的责任，对于台湾当局的政策、法令法规皆必须遵循外，对于自身也有严格的要求。陈怡宏处长表示：“在追求获利与风险的前提下，土银更强调对于风险的控制，举例来说，一家获利的分行，和一家虽获利但有操作风险或逾期放款的分行，管理层会更关注分行为何有操作风险或逾期放款的情况”。

“银行业务是高度仰赖信息科技的产业，因此面临更多元与诡谲的信息风险，一旦发生系统中断，不单只是信息单位的损失，对于业务的影响更剧。在此情况下，我们信息处面临如何协助将业务营运上非预期的状况和损失最小化的挑战，因此我会将管理重点放在致力确保信息服务的正常提供、最小化系统营运中断后带来的损失、及降低资料外泄的机率”，陈处长说。

管理重点一：以信息安全体系为基础，致力提供不中断的信息服务

为了提供稳定的信息服务，信息处首重上线作业的控制管理。银行过去的系统架构为大型封闭式架构，与外部网络介接甚少，因此着重在上线人员权责分离、档案访问权限的管理。随着业务的扩展，银行系统架构的日益复杂，陈处长表示：“看似简单的业务需求，往往涉及多支交易的调整，信息处人员虽然相当熟悉程序内容，但对于业务交易间的操作和关联性较不熟悉，可能导致上线后才发现交易有连动的状况，因此信息处对于测试作业的控制管理亦相当重视，以求及早辨识问题。随着信息处对于日常作业的持续改善，我们信息处现已透过系统控管整个需求、变更、测试流程”。

而随着全球化程度日深，土银也积极在海外布局，先后在六大国际金融都会设立分行，其中得益于两岸签订金融业MOU(金融监理备忘录)及ECFA(两岸经济合作架构协议)，土银上海分行也已于2010年12月开业；海外分行、大陆分行所使用的系统也由信息处统筹规划，目前信息处已完成海外分行系统的集中化，并将台湾地区分行、海外分行、大陆分行使用的网络、系统环境进行切割，陈处长表示：“目的就是为了避免系统间彼此影响，而造成系统的不稳定”。

管理重点二：建立灾备恢复机制，最小化系统中断带来的损失

虽然平日已经做好准备，但仍难保万无一失，因此信息处针对灾备恢复是“做真的”，包含透过DWDM、光纤技术进行在线同步数据的抄写，确保发生重大灾害时，所有系统的数据都有备份并可回复。做好了备份与灾备恢复，信息处的下一步是确保企业的永续经营，陈处长认为：“信息风险的控制与业务需求是息息相关的，在有限成本和资源下，需要透过公司高层从业务面决定那些是关键业务系统，再来谈灾备恢复与永续经营的策略”。

管理重点三：个人资料保护

在台湾，新版《个人资料保护法》通过立法机关三次的审议与表决，正式生效后，显示台湾当局对于保护个人资料的要求更加严格，不仅扩大适用本法的主体及于任何自然人、法人或其他团体，及保护客体，包含明确定义个人资料范围不再限于经计算机处理的个人资料，并要求企业搜集、处理或利用个人资料前，具有事前告知义务，并加重持有个资业者（拥有和处理个人资料的相关企事业单位）的保管责任；加上云计算科技与应用的成熟，无论是公有云或私有云的建置，对于拥有大量个人资料的银行业，责任和风险都较以往提高。

陈处长表示：“如果客户数据外泄，信息处必定是首当其冲，因此如何评估与保护个人资料对于信息处是相当重要的课题，不久的将来，我们将基于现有的信息安全体系，建构个人资料保护的框架，并计划取得BS 10012个人资料保护标准认证，以示土银对于个人资料保护的决心”。

管理挑战一：在有限资源与成本下，控制信息风险

随着业务发展和科技进步，土银的业务系统、主机、服务器日益增加。举例来说，服务器的数量从信息处迁移至现在的机房后至少成长50倍以上，但伴随而来的，其实是管理的难度增加。陈处长表示：“每个系统除了在系统架构、技术使用上有差异外，安全上的控管也略有差异，因此信息处已制订架构和作业标准，现在信息人员从一开始的系统规划、分析、开发测试、外包管理到后续运维，都有可依循的准则，以降低作业上面临的问题与风险”。

另一方面，为了要“Do more with less”，除了标准化作业，信息处也在精简管理和维运成本上下功夫，包含完成分行系统后台的集中化作业，并持续进行系统的集中管理。而集中化的下一步，就是透过引进新技术，降低信息人员管理的困难度和成本，和提供使用者更完善的服务。举例来说，引进虚拟化技术、负载平衡的管理后，以往各自系统要自己进行负载平衡，未来信息处就可以整体规划与管理系统负载平衡的架构，让资源使用更具整体性与规模经济；并透过建置桌面云、提供外部、内部人员使用的行动银行等，提供使用者更便利的服务。

然而，新技术的使用对于信息处亦是另一项信息风险，在土银稳健营运的原则下，信息处对于新科技的评估更为审慎，一旦决定采用，会进行充分测试，根据系统的重要性，分阶段实施，以确保在新技术带来的效益和风险上取得平衡。

管理挑战二：面对风险的处理方式

良好的信息风险管理包含了设计与建立风险管理组织与权责，进行风险识别与评估，尔后由相关权责人员进行风险控制与处理，并持续监督与改善。全面性风险评估是做好信息风险管理的第一课，陈处长表示：“在鉴别与评估风险的时候，要从业务面了解信息风险带来的影响，且要注意信息风险控制不能背离业务需求”。

因此他认为信息人员若只待在信息处内部，是不能够了解信息风险对于业务营运的影响，要真正去了解终端使用者如何使用，才能知道实际的风险在哪里，进一步再来谈是否能够处理、并处理风险。因此他除了多鼓励信息人员内部多沟通、主动了解业务外，也在内部进行职务轮调，让每个人用不同的角度看事情。陈处长以自己为例，过去他就曾经轮调过业务单位和分行，对于前线面临的挑战与风险就具有比较深刻的体会。

土银对于信息风险管理未来发展策略与规划为何？

对于土银信息处来说，安全永远是一个议题，对于安全的控管与防护，以往信息人员都是想到什么才去做，买了很多管理工具，缺乏整体的规划；面对未来发展的策略重点，陈处长表示：“目前已完成信息治理蓝图的规划，透过蓝图先了解总体需求再谈如何实现，举例来说，透过资安蓝图来谈如何进行数据保护，了解哪些是现在必须要有的、哪些是未来应该要有的，哪些是可选择的，排定规划，按照时程规划实施”。

而对于信息风险管理成效的展现及未来规划，陈处长表示：“土银信息处在2008年取得ISO 27001信息安全认证后，信息处期望能够在健全体质后，优化服务水平与提升客户满意度，下一步便是取得ISO 20000信息服务认证，并强化对于个人资料的保护(BS 10012)与确保营运持续经营(BS 25999)，藉此提供台湾土地银行海内外及大陆的分行更稳定、完善的服务”(注)。



受访者陈怡宏处长学经历：

- 政治大学财政系、美国东德州州立大学计算机系硕士。
- 1986年12月进入土银信息处，先后担任过经办、领组、副科长、科长，曾经轮调至联机管理科、数据管制科、程序设计科、电子金融组等科组。后来陆续在东台北分行担任副理、电子金融中心副主任、信息室副主任、内湖分行经理。目前担任土银信息处处长。

注：德勤台北事务所目前为台湾土地银行信息风险治理之咨询顾问。

2010年度全球安全调研报告

前言

新的十年对于我们这些与信息安全产业息息相关的人是一个转折点。我们如今生活在一个网络战争的时代，环境是如此的险恶。原本在各自地下室中搞恶作剧的孩童，如今已不再有资格上新闻了。他们被全职的计算机舞弊人员所取代，为政府或个人实施集团犯罪，这些犯罪的目的可以是获取金钱、可以是为取得不正当竞争优势、可以是为取得技术领先。国与国之间互相指责对方使用网络战。每一个规模巨大的网络都曾被某种方式攻破过，政府都在任命高级军官负责网络战。其间的利害关系从未如此高昂，战争在世界上每个角落展开。它们包括：僵尸网络、特洛伊木马、恶意软件、垃圾邮件、钓鱼，如今这些欺骗手段是如此复杂以至于最谨慎的人都可能被骗。

本年度的安全调研结果支持着这样一个事实，那就是行业转折点已经来到：

- 第一次，组织开始积极进取迎接新技术的到来，领先者不再满足，落后者迅即反应。
- 第一次，有最少比例的受访者（36%）表示“缺乏足够预算”是其确保信息安全的主要障碍，区别于去年的56%。即使在记忆中最严重的经济衰退中，即使有那么多预算被削减，大部分信息安全预算还是得到保障，许多部分还有增加。
- 第一次，信息安全合规性（内部/外部审计）整治成为前5位的安全措施，表明组织开始关注监管和立法。
- 第一次，有超过50%的组织表示纸张等物理信息，在其信息安全执行团队的执行任务和责任范围内。比例（59%）还是太低－表明存在一个安全缺口－但是我们认为方向是正确的。

我们谈论了许多日趋复杂的威胁。如今我们还有一些别的事要处理：竞争力水平的降低构成了威胁。蝴蝶（Mariposa），这个源于西班牙的僵尸网络影响了全球数以百万计的计算机。犯罪者们只拥有“有限的计算机技能”，却能够写出高明的计算机程序－他们只是简单地从互联网上下载所有想要的东西。一个新的现实是在互联网上可以使用的工具是越来越多，允许那些只拥有很少专业技术的人实施网络犯罪。

这是我们调研以来的第7年。很多人从重要而忙碌的工作中抽身为这些调研问题投入时间和精力，对此我向全球各金融机构的首席信息安全官、他们指定的代表、安全管理团队以及他们背后那些协助完成全球安全调研的人们表示我诚挚的谢意。没有你们根本无法做到这一切。

我们已经讨论了多年的变化。如今，我们站在这里，投入我们所有的智慧、知识和专业技能去进行并赢得网络战。这会是充满挑战、令人兴奋的，将有许多方面会取得进展。我们相信现在会是信息安全产业的黄金十年。

阿德尔 梅勒克 Adel Melek
德勤信息和技术风险全球领导人
DTT Global Leader, Information & Technology Risk
德勤企业风险服务全球金融服务行业全球领导人
DTT Global Leader, Enterprise Risk Services – Global Financial Services Industry

图1．调研对象地区分布情况

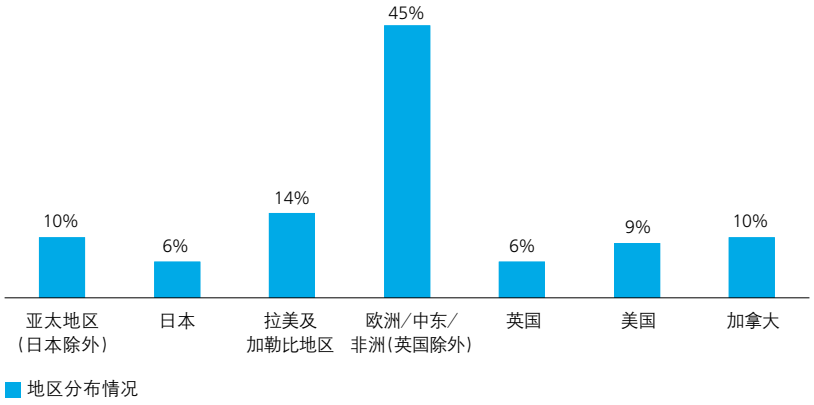


图2．调研对象年收入分布情况（美元）

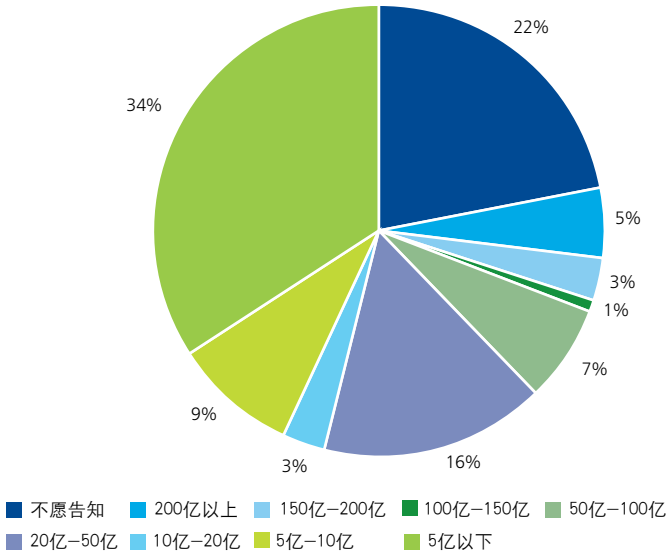
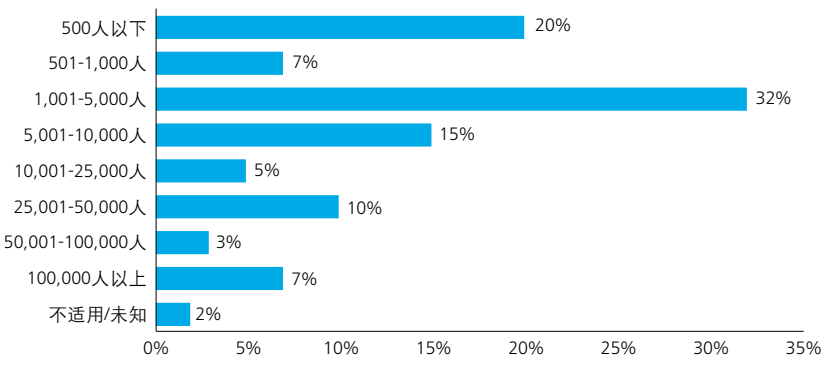


图3．调研对象公司规模



1．调研对象

2010德勤全球安全调研的目的是将德勤信息技术风险相关专业人士的研究成果与全球各行业安全风控专家的实际经验相结合，以更好地了解全球企业在信息安全风险管理方面的现状以及当前面临的挑战。

1.1按地区统计

本次调研参与企业遍及全球45个国家近千家（实际963家）公司，其地区分布情况如图1所示：

1.2按年收入统计

本次调研参与企业年收入情况分布较为平均，不仅有大型跨国公司，其中也包括规模较小以及规模适中的企业，上市与非上市公司分布较为均匀，其公司年收入如图2所示：

1.3按公司规模统计

为了更好地进行有针对性的数据分析，本次调研参与企业可按其员工人数划分为8类，其具体分布如图3所示：

1.4行业概况

参与调研的963家企业的行业分布主要集中在金融服务、技术媒体通信、快速消费品等，其中有350家为金融服务机构（Financial Services），146家为技术/媒体/通信类企业（TMT）。（见图4）

2.调研方法

本次调研首先要了解企业是如何处理信息安全问题的，具体来说又可细分为以下3点：

1.企业是如何结合其自身行业特点来识别风险的?
2.企业全员的风险意识水平如何?
3.企业是如何利用内部和外部资源来缓释/转移识别出的风险的?

其次，本次调研会进一步分析日新月异的技术发展对企业信息安全的利弊以及企业加大信息安全方面投入会带来的影响。

为此，德勤信息技术风险服务小组（Deloitte Information Technology Risk Services Group）的专家设计了本次调研的调查问卷，并对调研结果进行定性和定量的分析，以便于从宏观战略和微观运作两方面来更好地解读信息安全。

2.1调研问卷格式

在设计2010版全球安全调查问卷时，我们充分考虑了全球各行各业的实际情况，又在上一年度问卷基础上部分精简以便于参与者回答，同时又新增了部分媒体热点问题以体现时效性。

本次调研问卷包含2大部分：

1.核心部分－在综合考虑各行业实际情况后设计的问答体系；
2.特别部分－对于业务持续性管理和灾难恢复进程，单独设计了更详细更深入的内容。

2.2问卷数据汇总

本次问卷调研通过访谈、邮件、电话等形式进行，问卷对象主要是各企业的首席信息官（CIO）、首席技术官（CTO）、首席信息安全官（CISO）或其代表，收集的所有数据会按地区汇总至德勤各地区总部，并最终提交给全球安全调研团队。

2.3统计分析方法

德勤信息技术风险服务专家根据各行业的最佳实践情况分析本次调研的结果，分析数据时根据统计学原理对数据进行了离散值修正，因此部分答案未包含在统计结果内，以确保分析结果简明直观。同样，本报告部分图表统计结果合计不足100%，也是由于去除了部分答案。此外本次数据统计不包含未作回应的问卷。（见图5）

图4．调研对象行业分布情况

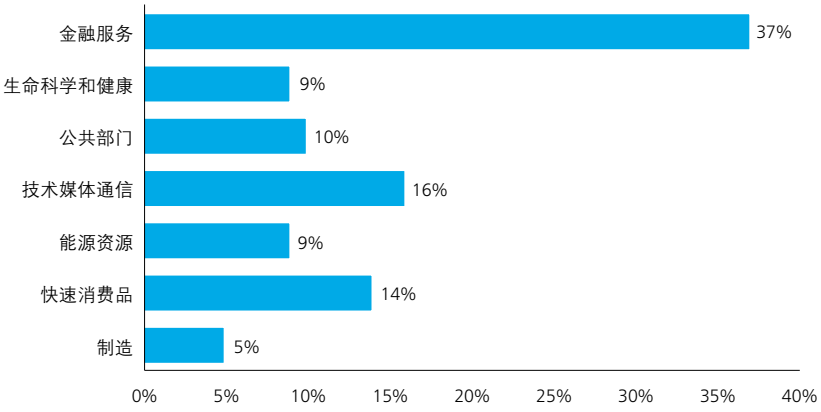


图5．图表解读情况

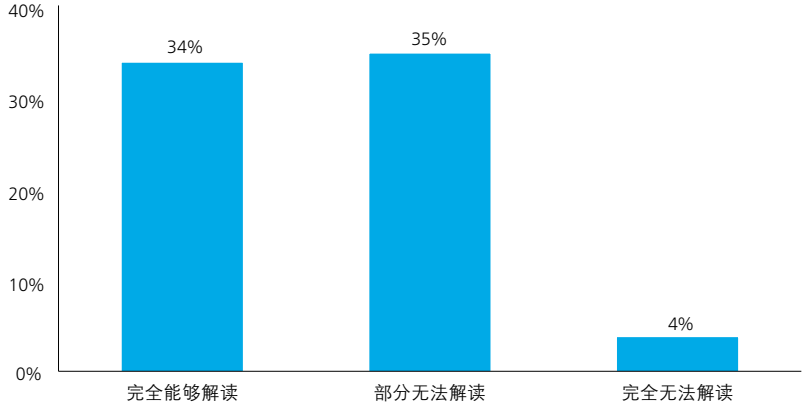
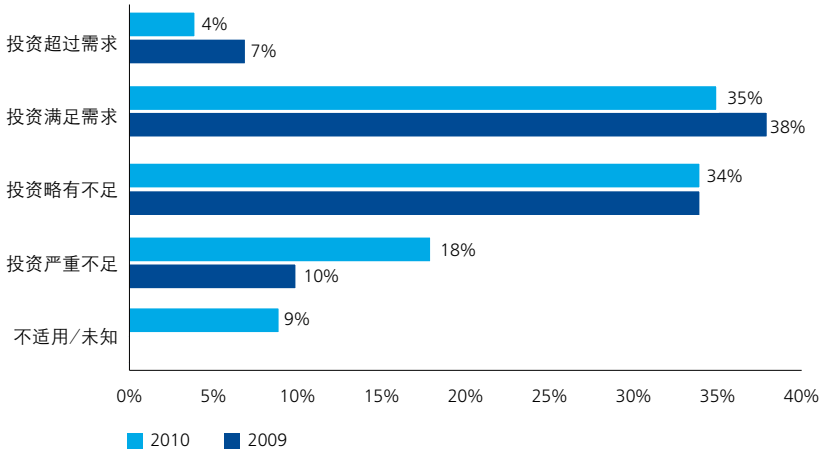
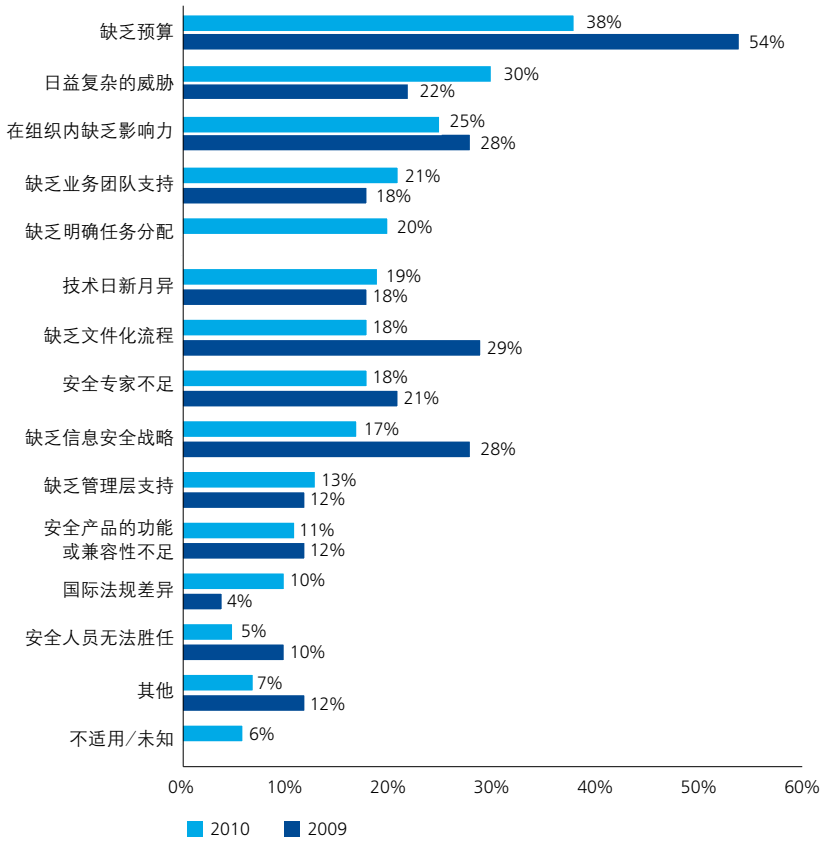


图6．信息安全投资



注：2009年未统计“不适用/未知”的数据

图7．组织面临的信息安全主要障碍



注：2010年调研中新增“缺乏明确任务分配”的调查内容；且2009年未统计“不适用/未知”的数据

3.调研结果

3.1信息安全投资

在2009年全球安全调研中，由于当时正处于世界金融危机中，企业都在想尽一切方式削减成本，安全投资方面也不例外。上一年度预算削减的影响充分体现在本年度的回应中，只有4%（2009年7%）的企业认为信息安全投资超过需求，35%的企业认为投资基本可以满足需求（2009年38%），而有52%（投资略有不足34%，投资严重不足18%）的企业认为信息安全投资无法满足需求以应对各类安全威胁，而2009年只有44%受访者这样认为。（见图6）

通过本年度调研，预期经济恢复后企业对安全领域投资有所增加。在经过1年的省吃俭用和项目延期后，一些重要的安全项目和基础设施升级将要实施。2010年调研显示，尽管过去2年受金融危机影响企业对于预算安排更加严苛，但是把“缺乏足够预算”视为企业面临主要障碍的受访者同比有所减少（今年是38%，2009年是54%）。随着信息安全环境日趋复杂，数据保护方面的投入也日趋增大。因此，企业为实现更高的投资收益率必然要求安全方面万无一失。根据调研结果，2010年投入较大的部分有身份识别和访问控制管理（IAM）、安全基础设施升级、监管和立法规定以及信息安全合规整改。（见图7）

另一点值得注意的是，信息安全预算较2009年同期有所增加。有9%的受访者表示预算同比增加超过10%，43%的受访者认为预算同比增加0－10%之间。此外，认为其信息预算被削减的组织大幅减少至20%。（见图8）

尽管存在全球性衰退和业务复苏缓慢的情况，还是有30%的受访者认为他们的业务开展与信息安全很好地结合，59%认为业务开展与信息安全基本能够结合，同比略高于2009年的28%和55%。同时，认为两者无法结合的受访者从2009年的15%锐减至6%。这些数据表明，企业正尝试更明智地使用其安全预算，从而能够以更合理的成本达到较高的安全水平，以在未来立于不败之地。（见图9）

图8．预算同比变化趋势

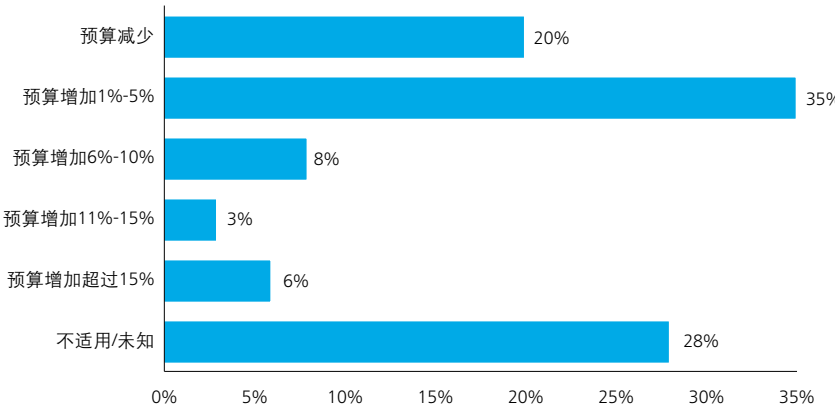
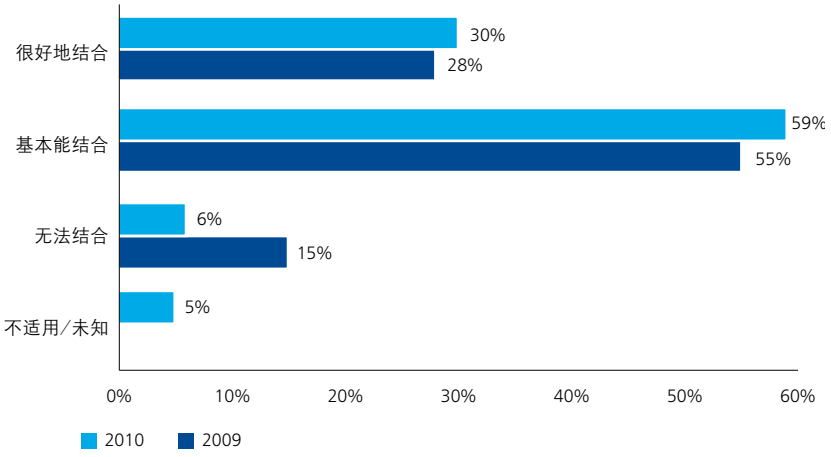
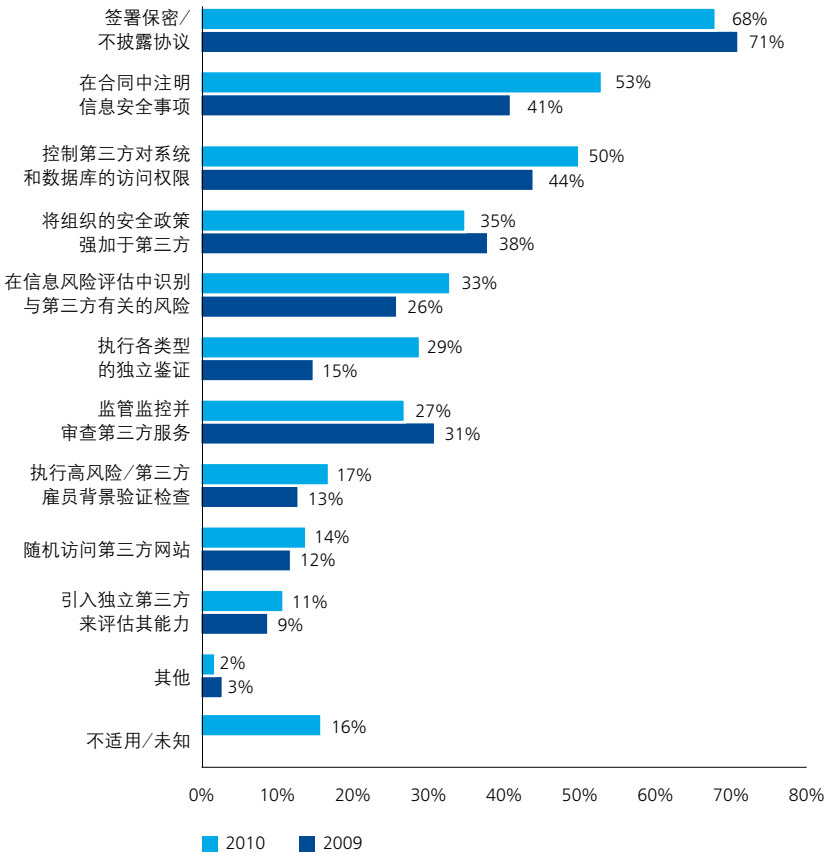


图9．业务开展和信息安全的结合程度



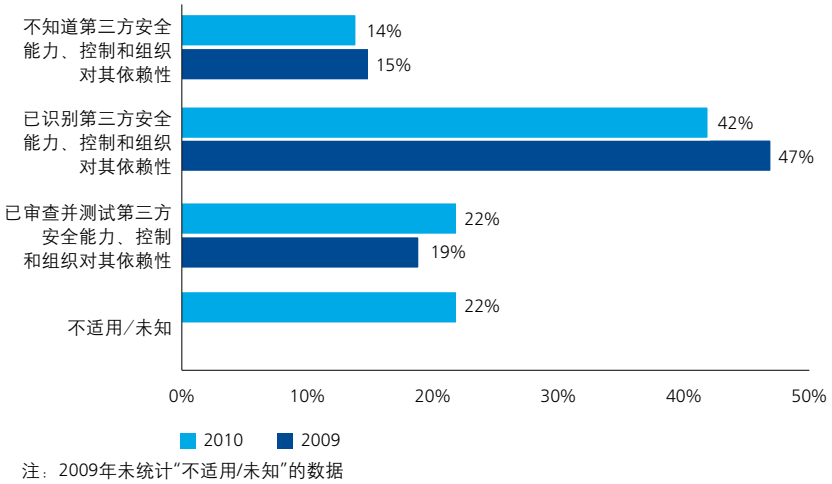
注：2009年未统计“不适用/未知”的数据

图10．第三方安全实践



注：2009年未统计"不适用/未知"的数据

图11．第三方安全能力、控制和组织对其依赖性



注：2009年未统计"不适用/未知"的数据

3.2第三方供应商安全能力

现今几乎没有什么业务能由企业单打独斗完成，绝大多数业务需要企业与客户、供应商及其他第三方共同配合完成。在这样高度分散和复杂的价值链中确保信息安全，要远比在单独组织内保护信息安全来得有挑战性。

管理一家外部的业务合作伙伴与管理一个内部的业务部门是完全不同的。根据我们的研究，这一调查结果和2009年基本相同。最普遍的方法是"签署保密/不披露协议"（68%），其他通用方法包括"在合同中注明信息安全事项"（53%）和"控制第三方对系统和数据库的访问权限"（50%）。（见图10）

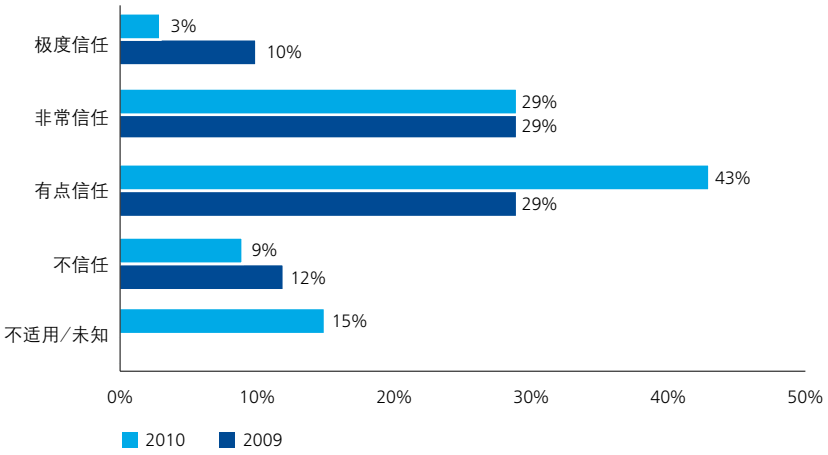
有效的安全需要的不仅仅是协议和合同。鉴于安全和隐私的重要性日渐增加，攻击威胁也逐渐升级，组织都在争先恐后地确保其业务伙伴的安全功能是最新的和得到验证的。研究表明有64%的组织曾经识别过其业务伙伴的安全能力，然而其中只有22%被实际测试过。有14%的受访者表示他们根本不了解业务伙伴拥有怎样的业务安全能力水平和安全控制。在此环境下，这一问题可能使组织处于危险境地，因此再也不能得过且过，而应立即予以重视。（见图11）

尽管缺乏测试和验证，依然有32%受访者对其第三方高度信任，有43%基本信任，只有9%选择不信任第三方合作伙伴。（见图12）

更严格的安全规章会促使组织在此问题上采取行动。然而，只有规章制度是不够的。大多数的规章制度的制定需要建立在物理业务模型的基础上而不是网上业务模型上。根据调查，有53%的组织认为已经从高级管理层得到充足的承诺和资金以有效地满足监管和法务要求，这与去年相比有一定提高（2009年42%）。然而与去年相同，大多数受访者认为监管要求充其量只是略微提升了企业的信息安全水平。（见图13）

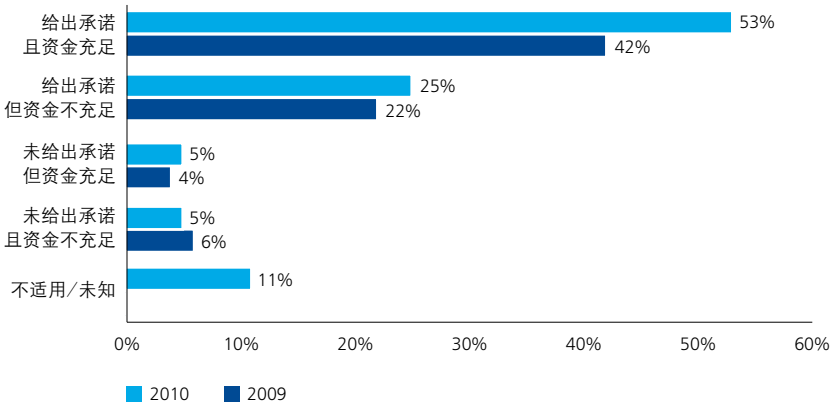
此外，根据调查企业在业务连续性方面雇用第三方主要是异地储存数据（36%）和使用灾难恢复设施（33%），外包供应商提供业务连续性管理软件的相对较少（9%）。（见图14）

图12．第三方信任程度



注：2009年未统计“不适用/未知”的数据

图13．监管安全要求



注：2009年未统计“不适用/未知”的数据

图14．业务连续性相关第三方服务类型（2010年）

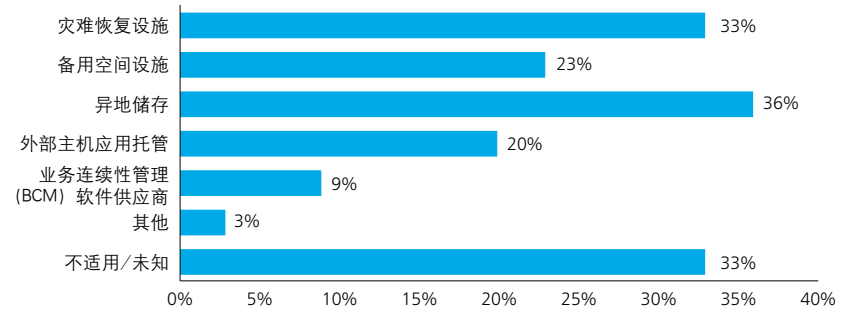
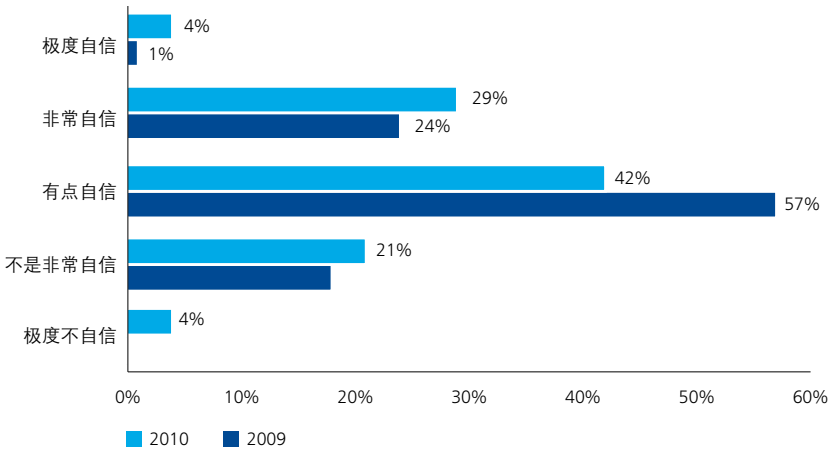
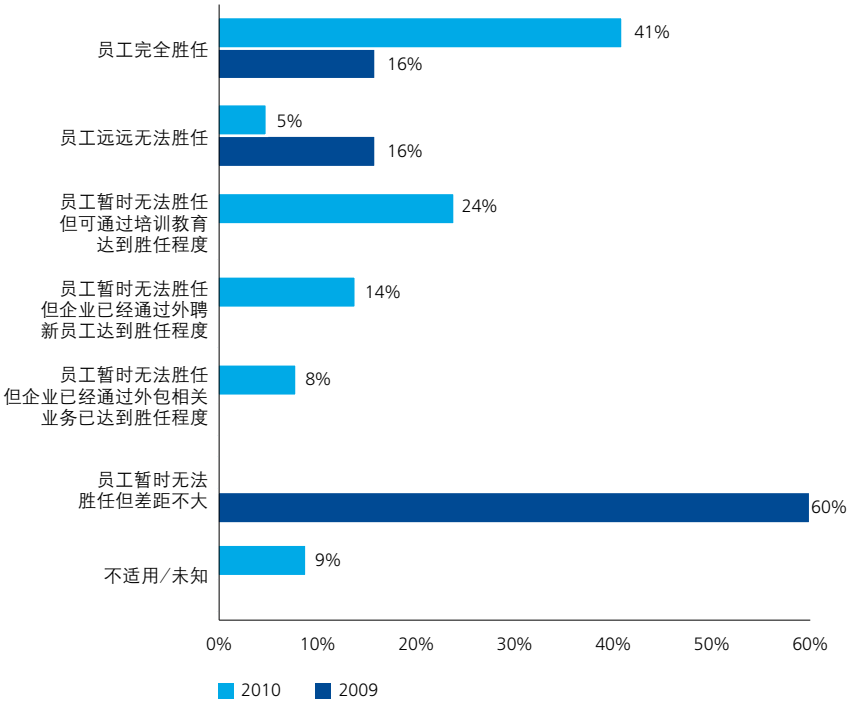


图15．处理源于内部的攻击



注：2010年新增"极度不自信"选项，2009年无该项数据

图16．员工胜任能力



注：2009年将"员工暂时无法胜任"设为1个选项，2010年分为3个选项；
同时2009年未统计"不适用/未知"的数据

3.3人才培训和教育

人才是企业成功的基石。组织应当更关注与人相关的安全问题，尤其是对于内部漏洞更是如此。内部安全挑战日趋严峻，这都要感谢移动设备、无线网络和社交媒体的普及。如今，大多数员工人手一台笔记本电脑外加智能手机，这便于其能够任何地点工作并接入互联网。不幸的是，远程工作员工的风险防范意识远远跟不上技术进步。

员工更容易泄漏敏感商业信息而没有意识到其行为后果的严重性，潜在问题包括遗失笔记本电脑、不慎分享敏感信息等。

根据我们的调查发现，组织对于自己有能力应对内部挑战充满信心。今年，有33%的受访者对自己有能力处理内部威胁极度自信或非常自信，而去年为25%。（见图15）

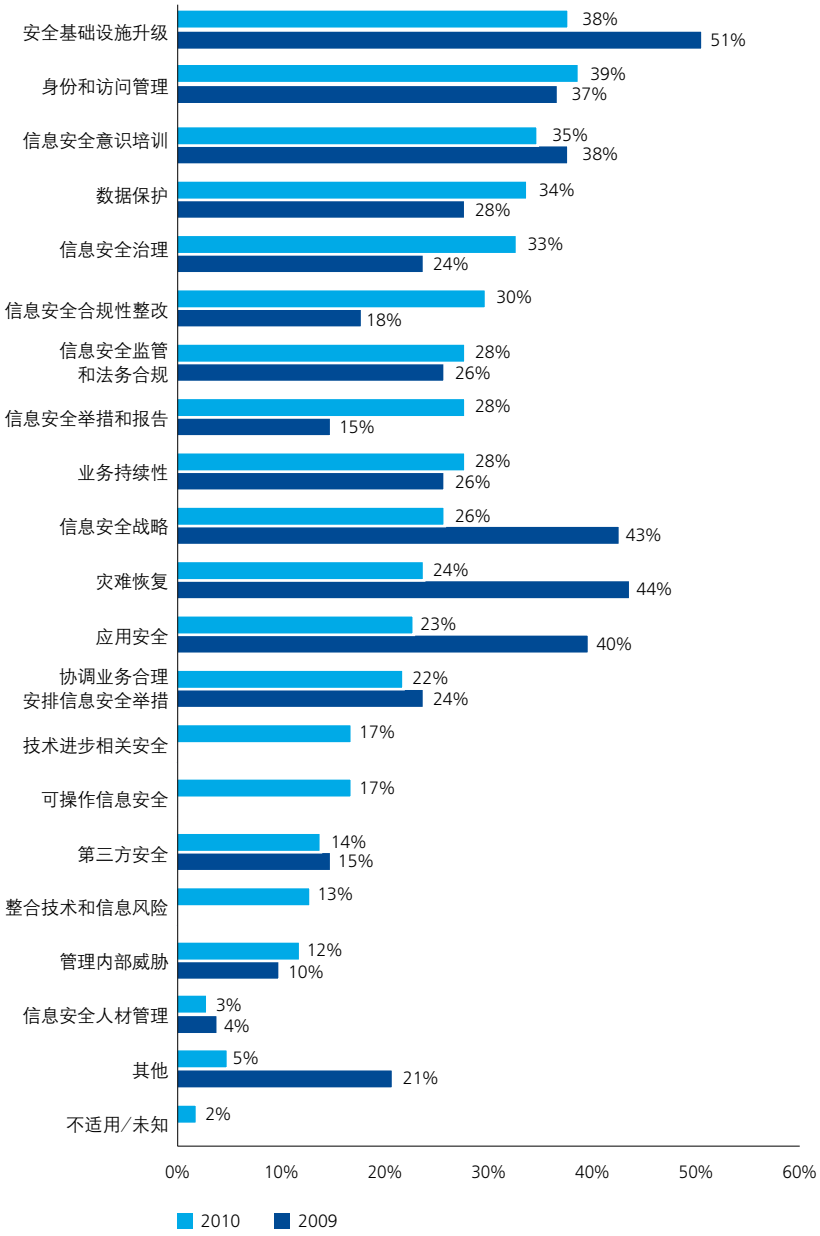
不过，还是有许多企业对于内部安全缺乏信心。几乎一半的组织承认，在过去1年中至少遭受了1次内部攻击，有50%的受访者认为其信息安全雇员无法胜任现有的和预期的安全要求。（见图16）

组织都在试图通过培训和发展来提升员工的能力。事实上，信息安全意识的提高和培训一直以来都是企业实施的主要安全举措，今年有35%的企业计划组织员工参加培训以提升其鉴别可疑活动的能力。同时，根据调研结果发现2009年排名前3的安全举措是“安全设施升级”、“灾难恢复”、“信息安全战略”，而2010年排名前3的是“身份和访问管理”、“安全设施升级”、“信息安全意识培训”。比较后我们发现，2010年在企业心目中信息安全意识培训的重要性正在加强。

值得注意的是在大多数企业其管理人员和第三方承包商并不接受专门的培训，这可能限制他们成为安全意识标兵的能力。多数安全意识计划始于在线学习模块，这可以提升风险意识并拓展知识背景，但是不足以影响其行为习惯。对于社交工程等越来越严重的威胁，专业的有针对性的拓展训练十分必要。

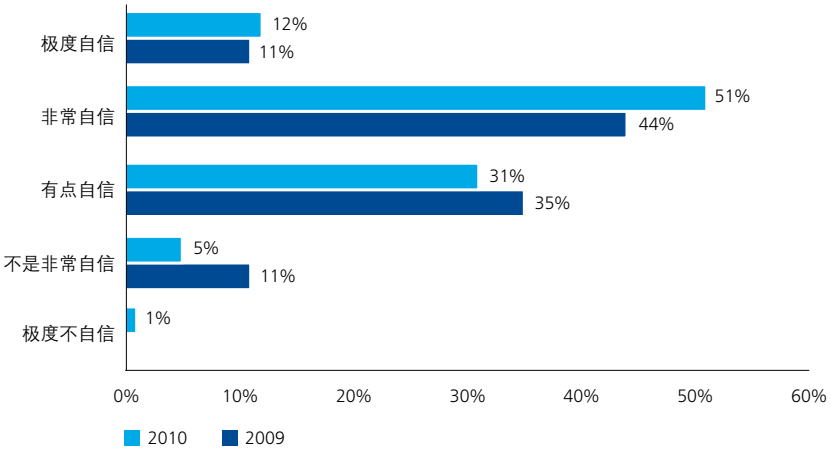
除了培训，还可以使用例如数据保护等其他技术和方法以降低对人员判断的依赖，确保达到更高的安全水平。在今年调研中，数据保护是排名前5位的安全措施，这表明受访者认可数据保护是其最优先采取的安全举措之一。（见图17）

图17．组织常用信息安全举措



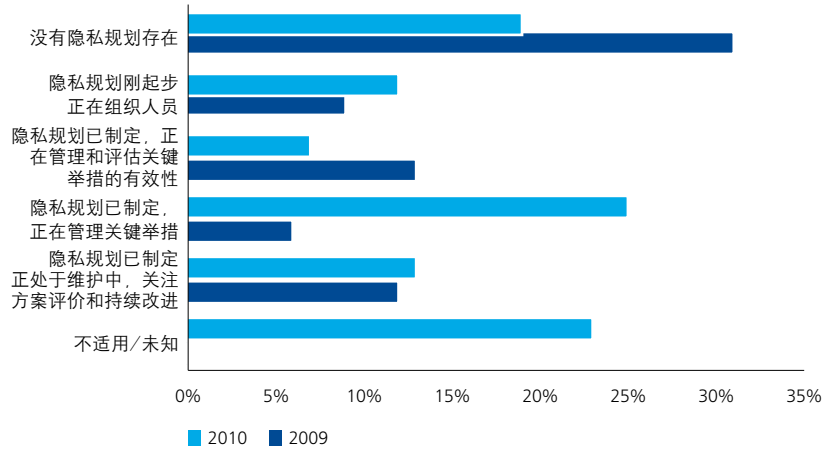
注： 2009年与2010年部分选项有差异，因此部分选项只有单一年份数据

图18．处理源于外部的攻击



注：2010年新增“极度不自信”选项，2009年无该项数据

图19．组织隐私规划成熟度



注：2009年未统计“不适用/未知”的数据

组织在处理内部攻击和外部攻击时产生了一个有趣的差异，有63%的受访者对于处理外部攻击是“极度自信”或“非常有自信”，而且这一数字相比2009年还有所上升（55%），这表明全球企业都意识到外部攻击是一个重大威胁，但似乎对于其自身具备的能力有点过于自信。其实处理外部攻击并不容易，举数据丢失防护为例，首先要从现有数据中区分哪些信息需要防护，分别需要何种层级的防护，其数据所有人又是谁，这些都是耗费大量时间、金钱、精力的大工程。（见图18）

3.4 信息隐私

几年前也许很难想象美国总统会如此关注信息安全而如今这已经成为现实。回顾往昔，计算机攻击通常是孩子们无所事事时的消遣和把戏，最严重的后果不过是被痛骂一顿。

时光飞逝至2010，美国总统奥巴马将网络防御当成国家的头等大事之一。美国政府已经任命了专职的国家网络协调员。北约也成立了网络防务合作卓越中心（CCDCOE）。这些行动表明网络恐怖分子的职业正在形成，网络犯罪已经专业化。

有30%的受访者将日益复杂的威胁视为其有效信息安全实现的主要障碍，仅次于缺乏足够预算的38%。尖端技术开发企业经常会无奈又无助地发现他们耗尽心血研发的技术和设备被用来实施网络犯罪或网络恐怖主义。通信运营商会发现他们的网络被不正当使用，他们的客户被僵尸网络绑架；媒体机构则面临邮件勒索，若不汇款至指定帐户其网上频道将会崩溃。全球组织都意识到技术进步会带来安全隐患，但如果没有切实有效的事前规划一切都是空谈。根据我们调研，只有45%的企业存在信息隐私规划。

因此可以很容易地得出结论，如果对这些威胁不制定有针对性的策略规划，将不仅影响到企业还会波及整个社会。我们可以想象如果电话系统和互联网络突然崩溃，或者个人隐私和机密信息暴露在全世界面前，这会是怎样的一番场景。（见图19）

3.5 地域影响

前文中我们针对全球的整体数据做了一些趋势和对比分析，但是在个别地区，信息安全实施的成熟程度还是有不小的差异。下面我们举金融服务业的调研结果为例，来说明地域不同对安全时间的影响。（见图20）

图20.安全实践的地理因素影响

	2009全球	2010全球	亚太地区（日本除外）	日本	拉美及加勒比地区	欧洲中东非洲（英国除外）	中东	英国	美国	加拿大
受访者表示信息安全执行报告提交给首席信息官CIO	33%	24%	22%	0%	18%	26%	20%	15%	45%	24%
受访者认为得到足够承诺和资金以满足安全监管要求	59%	62%	74%	30%	48%	64%	61%	60%	74%	71%
受访者表示存在成文的且经过审批的信息安全规划	61%	60%	71%	65%	54%	61%	47%	50%	55%	56%
受访者认为信息安全与业务开展已很好地结合	32%	37%	56%	35%	34%	35%	38%	40%	33%	35%
受访者表示信息安全预算已经得到增加	60%	56%	56%	16%	64%	53%	56%	70%	56%	76%
受访者表示信息安全投入大于或等于计划需求	43%	45%	50%	40%	58%	41%	27%	50%	30%	53%
受访者认为内部员工能胜任现有的和未来可预见的安全要求	34%	45%	49%	20%	37%	50%	42%	45%	45%	44%
受访者表示企业存在1人或1人以上专人负责隐私问题	57%	53%	37%	100%	30%	42%	11%	60%	77%	71%
受访者表示存在隐私合规性管理相关的计划	48%	50%	44%	95%	24%	44%	17%	55%	70%	71%
受访者表示已教育员工识别举报可疑活动	71%	64%	83%	35%	62%	59%	58%	75%	82%	62%
受访者表示已将身份验证和访问控制管理纳入其2010优先开展计划	54%	44%	42%	65%	38%	35%	15%	35%	67%	62%
受访者对其现有第三方安全实践非常自信		36%	29%	90%	40%	33%	35%	15%	6%	41%
受访者对其移动设备实施彻底加密		44%	42%	50%	12%	42%	13%	80%	61%	65%
受访者表示已维护损失事件数据库		54%	53%	70%	43%	52%	40%	79%	68%	44%

高分值　低分值

2010调研报告第一次单独统计了中东数据，以便于对中东地区有更好的了解。同时，日本虽然是亚太地区国家，但由于其经济发展状况不同，在此也被单独统计。通过上表，我们可以发现企业安全执行情况与企业所处地理文化环境密切相关。

1）我们发现在美国首席信息官（CIO）最得到重视，有45%（全球24%）的受访者表示其企业会提交信息安全报告给首席信息官；而在日本报告几乎从不提交给首席信息官。这也许是因为美国是全球最先推广在高级管理层中设立独立首席信息官的国家，而在日本可能由于文化理解、企业结构差异设置独立的首席信息官的企业较少。同时，我们也发现2010年这一数据（24%）相比2009年（33%）有所降低，这也许是因为2009年世界金融危机，使得多数企业更重视降低成本而对信息安全报告和首席信息官短期内缺乏重视。

2）我们发现在除日本外的亚太地区，有74%（全球59%）的受访者表示得到足够承诺和资金以满足安全监管要求，与美国持平；而在日本却只有30%的企业这样认为。这也许是由于亚太其他国家有许多处于上升期的新兴企业，他们对企业更有自信，也更愿意投入更多的人力物力以满足安全监管要求；而美国则是一贯重视安全方面投入。同时，我们也发现2010年这一数据（62%）相比2009年（59%）略有增加。

3）我们发现在除日本外的亚太地区，有71%（全球60%）的受访者表示存在成文的且经过审批的信息安全规划；而在中东却只有47%的企业这样认为。这表明亚太企业的高级管理层对信息安全较重视，而中东也许因为家族企业比较多因此制定成文规划的企业较少。同时，我们也发现2010年这一数据（61%）相比2009年（60%）几乎不变。

4）我们发现在除日本外的亚太地区，有56%（全球37%）的受访者认为信息安全与业务开展已很好地结合；而在美国却只有33%的企业这样认为。这也许部分因为在亚太地区信息安全要求相比美国来得低，对业务的影响程度也较轻，亚太地区企业管理层也更相信能同时兼顾信息安全和业务发展。同时，我们也发现2010年这一数据（37%）相比2009年（32%）有所增加，这表明全球有更多人认识到信息安全与业务发展并不矛盾。

5）我们发现在加拿大，有76%（全球56%）的受访者表示信息安全预算已经得到增加；而在日本却只有16%的企业这样认为。这也许因为加拿大与美国一样一贯比较重视信息安全资金投入，而日本却更多地削减了安全预算。同时，我们也发现2010年这一数据（56%）相比2009年（60%）有所减少，这也许是由于企业为应对全球金融危机而削减了部分信息安全预算。

6）我们发现在拉美及加勒比地区，有58%（全球45%）的受访者表示信息安全投入大于或等于计划需求；而在中东却只有27%的企业这样认为。这也许是因为地域文化原因拉美地区受访者对自身安全计划更自信，而中东对于信息安全投入较弱。同时，我们也发现2010年这一数据（45%）相比2009年（43%）几乎不变。

7）我们发现在欧洲非洲中东（英国除外），有50%（全球45%）的受访者认为内部员工能胜任现有的和未来可预见的安全要求；而在日本却只有20%的企业这样认为。这也许是因为欧洲非洲企业更信赖其员工，而日本企业认为其安全需求更难达到而更愿意信赖外部专业人士。同时，我们也发现2010年这一数据（45%）相比2009年（34%）大幅增长，表明企业给予内部员工更多的信息安全方面培训教育也更愿意相信内部员工。

8）我们发现在日本，有100%（全球53%）的受访者表示企业存在1人或1人以上专人负责隐私问题；而在中东却只有11%的企业这样认为。日本在此项上的遥遥领先也许是因为其社会文化对隐私保护更重视也更愿意安排专人来处理这类敏感事务，日本政府于2005年4月正式实施《个人信息保护法》，对于隐私权保护的法律非常严格；而中东由于企业管理结构不同和文化差异的原因对隐私没有那么重视。同时，我们也发现2010年这一数据（53%）相比2009年（57%）略有减少，也许是因为金融危机让企业削减了部分隐私专员。

9）我们发现在日本，有95%（全球50%）的受访者表示存在隐私合规性管理相关的计划；而在中东却只有17%的企业这样认为。这也许也是因为对隐私重视程度不同造成的。



10）我们发现在亚太其他国家，有83%（全球64%）的受访者表示已教育员工识别举报可疑活动；而在日本却只有35%的企业这样认为。这可能是由于文化原因，日本企业员工更不愿意举报可疑活动，也更担心报告后会招致打击报复。同时，我们也发现2010年这一数据（64%）相比2009年（71%）略有减少，这表明举报活动后的保护还有待加强。

11）我们发现在美国，有67%（全球44%）的受访者表示已将身份验证和访问控制管理纳入其2010优先开展计划；而在中东却只有15%的企业这样认为。这可能部分由于美国企业更容易遭受全球性的黑客攻击，因此也更重视身份验证和访问控制。同时，我们也发现2010年这一数据（44%）相比2009年（54%）较大幅度的减少，这很值得关注。

12）我们发现在日本，有90%（全球36%）的受访者对其现有第三方安全实践非常自信；而在美国却只有6%的企业这样认为。这可能由于日本企业互相间的信赖感更强，而美国企业更愿意对第三方供应商进行独立考核。

13）我们发现在英国，有80%（全球44%）的受访者对其移动设备实施彻底加密；而在拉美加勒比地区却只有12%的企业这样认为。这表明英国企业相比拉美对信息泄漏更重视。

14）我们发现在英国，有79%（全球54%）的受访者表示已维护损失事件数据库；而在中东却只有40%的企业这样认为。这也同样表明英国企业对信息丢失的重视。

15）综上所述，亚太地区（日本除外）在信息安全的资金投入、计划制定、员工培训方面处于领先，但需要注意的是隐私保护方面还有待加强，拉美加勒比地区同样如此。而日本正相反，在资金投入和业务举报方面得分较低，而亮点则是隐私保护方面做的较好。拉美加勒比地区在信息加密上需要加强。欧洲非洲中东（英国除外）是全球最认可其内部员工有能力胜任各项信息安全工作。中东则在多项指标中落后，在信息安全方面需要加大公司战略上重视和物质上的投入。英国似乎特别关注信息加密和信息丢失后的恢复。美国更重视安全访问控制和向首席信息官的汇报，而在安全监管方面受到较大的压力。加拿大各项指标较平均，只在安全预算投入方面领先于全球。

上海事务所的高级顾问曹吉进行了本文的前言翻译以及数据整理。并感谢德勤信息和技术风险全球服务小组提供调研数据。

企业安保：介绍企业安保风险抵御系统（增强版）

翁培业 Paul Yung
德勤中国
企业安保管理领导人

前言

恐怖主义、地缘政治冲突、自然灾害、全球化、个人隐私与信息保护、流行性疾病、日益增长的客户与民众的期望值，以及其他全球性力量正在重塑企业安保，这为独立可靠的组织高级领导团队顾问－首席安保官（CSO）带来了挑战和机遇。企业安保的优先度已经逐渐提升至C层级和治理层级，并且与企业风险管理（ERM）逐渐整合。企业安保风险应当和其他风险类型一样，在ERM强有力的框架下进行监控、评估、管理，而不再是孤立地进行管理。

依据德勤专有的企业安保风险抵御系统（下称"FIBER"），所有的关键资产例如设施（Facilities）、信息（Information）、业务（Business）、员工（Employees）、声誉（Reputation）都应当在风险评估的初始阶段被识别，并衡量特定意外事件对5大主要资产类别的影响。

CSO还需要充分了解企业安保风险管理（ESRM）的深度和广度，成为业务推动人并协助所有利益相关方实施各类企业安保措施。企业安保计划应当是以威胁为导向，以风险为基础。企业安保风险评估方法应当与其面临的风险相一致，并用来分析威胁和漏洞，评估组织的风险，在企业范围内提出风险缓解的建议。

德勤的FIBER系统是一种基于资产的方法，它强调了基础安保计划即组织应当积极关注于声誉风险和保全。它们是：

- 物理安保
- 信息安保
- 人员安保
- 危机管理
- 业务持续性

企业安保和企业风险管理

组织必须突破孤立型的风险管理，而建立起一种企业整体范围的风险管理（ERM）功能以确保能够广泛地、系统地、专业地识别全面风险。作为业务推动，企业安保应当与整体风险管理框架进行整合，并更深地渗透进各类业务风险。对于整体的企业安保管理方法的需求正在逐渐增长。例如，IT安保的整合需要在ERM的框架下更贴近于物理安保以及其他公司安保职能。由于风险智能共享、协同进行决策、以及高级管理层对于战略风险的关注和监管，这样的整合对于保护组织的品牌和声誉尤其必要。

前任德勤CEO白礼德（Bill Parrett）也对企业安保和风险管理提出新的见解。在他的著作《哨兵CEO：展望后9/11世界的安保、风险和领导力（2007）》中，物理资产安全和其他主要安保事件例如流行性疾病、恐怖主义以及黑客都应当成为企业主管的首要考虑对象。ERM已经成为日益明显和重要的管理解决方案，对于日新月异日趋复杂的风险尤其如此。白礼德先生也意识到CSO已经成为公司组织架构图中一个新的高级管理层职位，并且在美国多家公司中正在迅速成为高级管理层的关键决策人和首席执行官的得力参谋。

企业安保风险抵御系统（增强版）

德勤的FIBER是一种实用的企业安保系统，可用来保护所有组织资产包括物理资产、人员安保、信息安保机制、危机管理以及业务持续性战略。该系统为保护5大财产类别提供了复合型的安全和保障－设施（Facilities）、信息（Information）、业务（Business）、员工（Employees）、声誉（Reputation）。

“FIBER的英文含义为“纤维”，其本质上是细胞壁，它为植物搭建架构支撑骨架，给予植物力量、支撑、弹性以面对狂风暴雨。它的一个主要目的就是为新生的胚芽提供一副坚实可靠的铠甲。”





根据该系统，安保是一种增值性服务它强调主动防御而不是被动御敌。所有的安保计划都应该基于威胁和风险的评估结果以及针对个人和设施要求的安保建议。安保人人有责。在专业和胜任的安保机制的领导和指引下，每个员工都需要保持警惕和积极的参与。运用关键保护原则“制止、侦查、延迟和响应”可以提供一种整体的安保风险应对措施。

企业安保风险抵御系统（增强版）表明，为了评估风险，后果分析应当要预测5大主要资产类别的潜在受影响程度。近期国际上一些知名的处理危机和应对失误不断表明声誉风险已经成为组织稳定的最大威胁，并对受牵涉的公司产生重大影响。例如，英国石油漏油事件、丰田召回事件。很明显，声誉风险并未完全与其他风险评估一并整合。危机中，业务领导层可能会过分关注其设施和业务所受到的影响而忽视了人员风险。例如，缺乏强有力的危机管理规划和团队会导致危机全面爆发并暴露在公众面前，最终演变成企业内部和外部的信任危机。

企业安保风险管理

企业安保风险管理（ERSM）的存在是为了确保那些传统上与安保相关却未包含进ERM的风险，能得到适当考虑和处理。为使ESRM成功，企业安保需要与其他控制职能无缝对接，例如合规和内部审计，以加强组织安保态势。在实施进程中，企业安保也需要与其他关键支持职能建立有效互动，例如人力资源、通信、法律、信息技术、安全以及设施管理。CSO不仅需要理解组织及其人员面临的安保威胁和安保风险，也应该积极了解业务运营、环境和事件的性质，以能够分析任何潜在的声誉风险的影响。组织应当关注如下关键领域以最大限度提升安保的价值并积极寻求安保风险的缓解：

- 物理安保
- 信息安保
- 人员安保
- 危机管理
- 业务持续性

此外，应当有系统的方法来获取和分析必需的风险智能信息以支持组织高级领导层实施资产保护和安保资源分配。一个企业的安保风险评估方法应当与其面临的风险相一致，并用来分析威胁和漏洞，评估组织的风险，在企业范围内提出风险缓解的建议。高级管理层也需要参与安保议题，并在风险全景导航中设定其风险偏好。

企业安保服务

更详细地说，下列企业安保服务是CSO应当关注的基本安保措施。

- 安保战略规划
- 对重要事件的安保规划
- 安保审查/能力评估/差距分析
- 安保分析评估
- 物理安保威胁和漏洞评估
- 紧急应对计划
- 危机管理计划
- 旅行安保计划
- 私人行政保护方案
- 流行性疾病应急计划
- 业务持续性规划
- 安保教育和提高认识讲习班/培训班
- 隐私与信息保护
- 企业调查
- 演习和演练

相关启示

本文的主要目的是阐述关于企业安保与企业风险管理的关系。开宗明义地论证应当在企业风险管理的大框架下妥善考虑对所有主要资产类别的整体保护，并介绍了“FIBER”的安保概念，即结果分析应当涵盖设施（Facilities）、信息（Information）、业务（Business）、员工（Employees）和声誉（Reputation）所受到的影响。同时论述了成功的企业安保风险管理最佳安保实践应遵循的顺序，并且详细地诠释了首席安保官在其日常职业生涯应当关注的主要企业安保措施。

未来的工作应当进一步完善相关内容并扩大其范围，以涵盖企业安保解决方案、企业安保方法论以及风险智能首席安保官计划，以有助于化风险为回报。

参考资料

- 《哨兵CEO：展望后9/11世界的安保、风险和领导力（2007）》，白礼德，2007－"The Sentinel CEO: Perspectives on Security, Risk, and Leadership in a Post-9/11 World", William Parrett, Wiley, 2007.
- 《整合物理信息安保与企业风险管理》，企业安保风险管理联盟，2007－"The Convergence of Physical and Information Security in the Context of Enterprise Risk Management", The Alliance for Enterprise Security Risk Management, 2007.
- 《企业安保风险管理：如何从大风险走向大行动》，ASIS，首席安保官圆桌会议，2010－"Enterprise Security Risk Management: How Great Risks Lead to Great Deeds", ASIS, The CSO Roundtable, 2010.

管控IT风险，提升IT价值
–2010年中国银行业信息科技风险管理年会主题演讲（文字稿）[1]

薛梓源　合伙人
石　凯　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，银行业务对信息技术的依赖程度日益加深，信息技术已贯穿于银行所有产品、流程和经营活动中，信息资源已经成为银行发展必不可少的重要生产要素。

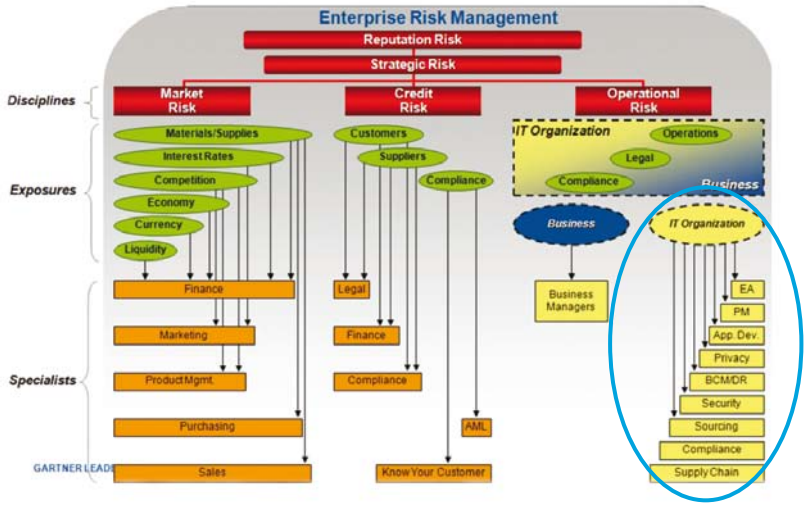
采取信息技术可以帮助银行快速响应市场需求、为客户提供高效率、高质量的服务与产品，但不断发生的信息科技风险事件使得银行管理层不得不考虑由于使用信息技术所带来的风险。如何识别与评估信息技术相关的风险，并通过一系列行之有效的机制进行合理地、科学地应对，提升银行信息科技的价值，是银行信息化建设以及全面风险管理建设所面临的新课题。

国际领先机构关于信息技术风险管理的观点

关于信息技术对于金融机构的影响，国际领先金融机构的CIO们早有深刻认识，例如卢森堡综合银行CIO迈克尔·道芬认为：

- 如果系统不可用或用户界面不友好，会对业务人员的效率产生影响；
- 由于系统不灵活，使得公司对新的商业机会不能做出快速反应；
- 数据支离破碎；
- 由于对用户接入管理不善，将导致欺诈行为的出现；
- 如果IT无法提供合适的报告方法，企业就无法按照法律要求进行充分的信息披露；
- 如果IT系统运转不正常，会使员工情绪紧张。

图1.IT风险管理在银行风险体系的一般定位



而美国银行认为，从引发信息技术风险因素的视角出发，信息技术风险来源包括技术过时、新兴技术、复杂的环境、内外部重大事件、监管制度调整、竞争力差距、业务模式变化和业务增长等，但总体可以概括为技术、业务和法律/合规三大来源，这些风险因素作用于银行各业务条线，形成信息技术风险，并对业务最终产生影响，体现在客户体验下降、IT支持能力降低、业务流程改进能力缺乏、市场响应速度滞后、业务决策分析受限、市场份额丧失等方面。

作为国际领先专业服务机构，德勤一直致力于全面风险管理的研究。 在德勤为金融行业制定的风险智能地图中， 信息技术风险是治理、战略和规划、运营和基础设施、合规和报告五大类风险之中运营和基础设施类的一种。 但是，通过更深入的分析各大类风险下的具体风险点，我们发现信息技术风险还包括为支持和实现信息技术运作而关联的其他风险。

信息技术风险管理的演进路线及发展趋势

信息技术风险管理在银行风险体系的一般定位（图1）

一般而言，银行需要建立一个全面的风险视图，作为其全面风险管理的基础。国外领先的银行的风险体系框架一般包括声誉风险，战略风险、市场风险、信用风险、法律风险、合规风险和操作风险（某些机构将法律风险、合规风险纳入到了操作风险中）。

1. 2010年10月27日，企业风险管理服务合伙人薛梓源参加了“第一届中国银行业信息科技风险管理年会”。并就《管控IT风险，提升IT价值》进行演讲。此文章为本次主题演讲的文字稿。

大部分国外银行的风险体系框架中，信息科技风险是操作风险的重要组成部分；在国内，随着信息化在银行经营管理中的作用和地位不断提升，一些国内金融机构则倾向于将信息科技风险从操作风险中单独列出。

信息技术风险管理的发展和演变规律

从以往信息安全管理到信息技术风险管理的发展来看，信息技术风险管理逐步从技术导向的风险管理到信息技术风险管理向融合化和智能化演进（见图2）：

- **技术导向的风险管理**
  通过采取技术手段来对IT资产进行防护是这个阶段的主要特征。
- **全面信息安全管理**
  建立信息安全防御体系和注重信息安全管理策略和流程是这个阶段的主要特征。
- **信息技术风险管理**
  基于业务价值和IT生命周期，全面考虑IT规划、建设、运维过程的风险管控和价值管理是这个阶段的主要特征，（信息技术风险也包括信息安全风险）。
- **信息技术风险管理的融合和智能化**
  信息技术风险管理同企业风险管理（ERM）的全面融合以及智能化的信息技术风险管理体系是这个阶段的主要特征。

信息技术风险管理的发展趋势

综合分析国际领先机构关于信息技术风险管理的观点以及信息技术风险管理的发展和演变路径，我们发现向企业风险管理的（ERM）全面融合和智能化是信息技术风险管理的终极目标。

一个风险智能型企业从风险治理、风险架构和风险过程层面都融入信息技术风险管理的考虑和设置。信息技术风险智能型的企业需要关注（见图3）：

- 将风险管理过程应用到IT部门即：识别、评估、管理和汇报IT相关的风险。
- 在企业范围内如何应用信息技术帮助其他部门识别、评估、管理和汇报有关风险。
- 信息科技领导人如何参与领导决策，确保战略风险得到适当的考虑，并帮助董事会理解企业面对的风险（包括信息技术风险）。

企业可以从IT风险智能管理体系取得的收益包括：

1. 风险智能的决策：帮助决策者理解决策制定的原因和风险相关的决策选项。
2. 一致的风险和控制视图：通过统一的流程，从风险治理实体的角度以一个统一的视图审视组织的各个部门。

图2.IT风险管理的发展和演变

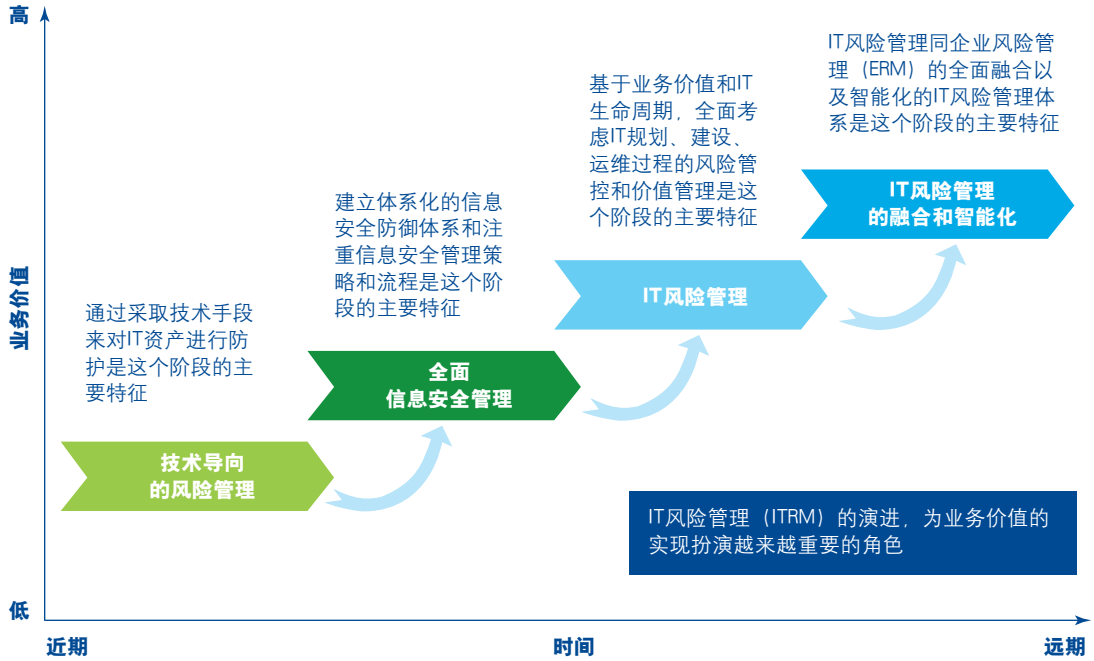


图3.IT风险智能型企业



3. 流畅的汇报渠道：以往没有风险趋势分析，并经常有延时的情况得到改善，现在具备了趋势分析能力和快速汇报能力，并且能够提供高质量的可靠的风险信息。
4. 基于工具的工作流：从以往采用电子表格花费上百小时降低到采用通用数据库和数据定义系统，花费时间大大缩短。
5. 可追溯的需求：从以往的领先实践的堆砌进化到监管实体与控制目标的有机整合。
6. 降低复杂性：减少大量汇报实体和冗余繁琐的流程。
7. 运营灵活性：实现从机械的风险管理到灵活的智能管控的转变。

信息技术风险管理如何适应“以客户为中心”的经营模式

在银行领域，“以客户为中心”的经营模式对管理信息技术风险提出了新的挑战。信息技术风险管理要提升银行的业务价值，需要适应“以客户为中心”的经营模式。

决不能将“以客户为中心”仅仅作为一句口号。从银行服务的角度看，“以客户为中心”要根据客户对金融业务的不同需求，实行专业化经营，系统化管理；银行不仅围绕客户做业务，而且还要围绕客户管理业务，包括经营管理、组织架构、业务流程都要以客户为中心进行设置。所以从银行经营与管理理念上要真正树立“以客户为中心”的经营思想，在银行营销策略上要认真贯彻“以客户为中心”的经营方针，在具体银行信息技术目标上要充分体会“以客户为中心”的功能需求。

面对“以客户为中心”的经营模式，银行的信息科技风险管理要以业务需求为导向，具体分析信息技术需求。例如，“以客户为中心”的经营理念，要求对客户群体进行细分，并进行定向销售；在具体技术实现上，客户信息数据需要实现集中管理，为科学分类提供依据；客户信息数据集中管理会让银行面临数据可用性、数据保密性、数据完整性以及客户隐私保护等风险。为了能快速响应越来越多的客户个性化需求，银行的软件开发要能快速实现客户需求的软件系统，信息科技风险管理就要关注开发过程中的风险以及软件系统自身的安全风险。为确保IT服务持续、快捷，信息技术风险管理就要关注IT业务持续风险。

银行业务上的变革，都对信息技术风险管理提出了新的挑战：

- 如何将信息技术风险融入银行全面风险管理体系，以确保IT更好地支持“以客户为中心”的银行经营活动？
  - 如何确保信息技术风险管理治理架构符合“以客户为中心”的银行治理架构？
  - 信息技术风险管理策略应如何体现“以客户为中心”的指导思想？
- 如何以保障客户良好体验为IT目标，有效地从全局角度管理信息技术风险？
  - 如何通过常规化的信息技术风险评估机制识别影响“以客户为中心”目标实现的问题？
  - 如何实施信息技术风险控制措施，将已知风险控制在可接受的范围？
  - 如何构建信息技术风险监测机制，将信息技术风险监测工作规范化、日常化？
  - 如何实现信息技术风险管理工作的持续改进？
  - 如何借助信息技术开展信息技术风险管理工作，提高信息技术风险管理工作的自动化程度？

银行业信息科技风险管理者只有积极应对上述挑战，才能最大程度上提升IT和业务价值，帮助实现银行战略目标。

建设有效信息技术风险管理机制的方法和关键要素

为了适应“以客户为中心”的经营模式，德勤提出了建设有效信息技术风险管理机制的方法。德勤为建设有效的信息技术风险管理机制制定了方法论，该方法论覆盖了信息科技风险管理的全生命周期（见图4）：

1. 建立信息技术风险管理治理架构：明确负责信息技术风险管理相关机构、部门职责与岗位，并制定合适的信息技术风险管理策略 。
2. 建立信息技术风险管理框架：依据最佳实践、监管要求和银行实际情况建立风险框架和风险数据库 。
3. 信息技术风险管理评估：了解银行信息技术风险管理现状并进行风险评价 。
4. 信息技术风险应对：依据风险评估结论，设计信息技术风险应对解决方案，并进行实施 。
5. 监控信息技术风险管理绩效：设计信息技术风险管理监控指标体系，并持续监控 。
6. IT审计与持续改进：通过独立审计发现信息技术风险管理的问题，持续改进 。
7. 通过信息技术风险管理技术手段对风险管理工作流和风险管理数据的统一管理，支撑信息技术风险管理的融合和智能化 。

建立信息技术风险管理治理架构

建立良好的信息技术风险管理治理架构是有效开展信息技术风险管理工作的基础，国内外银行都在建设信息技术风险管理的三道防线，三道防线必须共同合作，鉴别和管理各业务单位内部和整个公司的风险才能有效发挥防范作用。以国外某银行风险管理治理结构为例（见图5）：

第一道防线 ：业务单位经理负责鉴别、评估、承担和控制与各条线相关的风险。

第二道防线：全球合规和操作风险部门及其他辅助职能部门（如运营部门、技术部门和风险部门）与业务单位共同鉴别、评估、承担和控制所有风险，独立运行。

第三道防线：稽核/审计部门，对信息技术风险管理控制措施进行独立的测试、验证和评估。

图4.建设有效IT风险管理机制的方法论

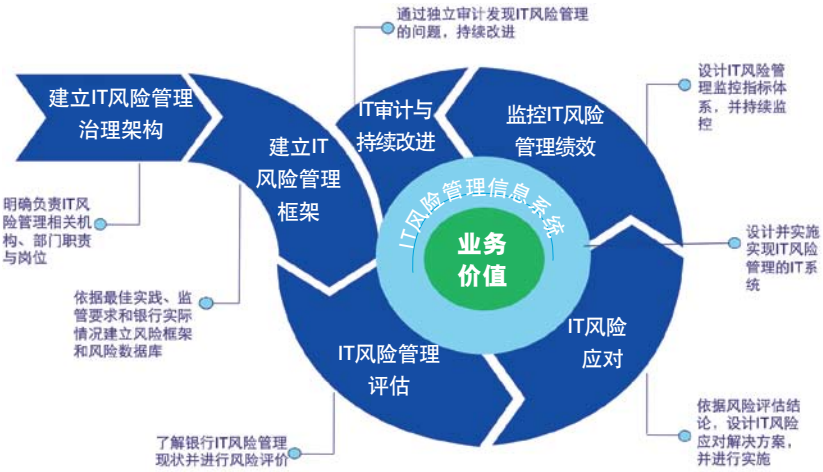
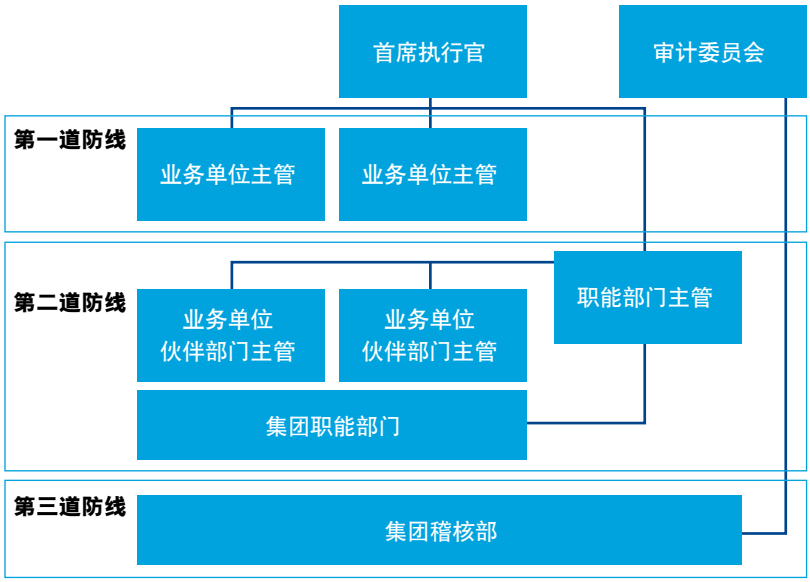


图5.国外某银行风险管理治理结构



通过设计合理的信息技术风险治理，应该在全行范围内明确信息科技风险管理涉及角色的不同工作职责以及各角色相互协作的方法，包括风险管理委员会、信息技术委员会、审计委员会的职责分工，以及CIO、信息科技部门、风险管理部门、审计部门、法律合规部们、人力资源部门等相关人员在信息技术风险管理各环节的职责和分工等内容。

建立信息技术风险管理框架（图6）

信息技术风险管理框架指导银行开展信息技术风险管理的整体活动，银行需要参照领先实践制定适合自身特点并符合相关标准的信息技术风险管理框架，目前国际上对于信息技术风险管理的相关的领先实践比较多，包括AS/NZS 4360、ISO27005、IRM RMS、COSO ERM以及ISACA的Risk IT。德勤综合分析这些领先实践，制定了德勤信息技术风险管理框架，该框架包括风险治理、风险策略、风险评估、控制活动、信息与沟通以及监控报告6个部分。德勤已经运用该框架帮助多家银行进行信息科技风险管理的实践。

信息科技风险管理框架

风险管理内容

风险治理	风险策略	风险评估	控制活动		信息与沟通	监控与报告
信息技术领域						
风险管理组织	信息科技战略	风险识别	IT组织和人员	运行体系	沟通策略	内部监控程序
经营环境	IT风险管理策略	风险分析	IT制度建设	操作环境控制	信息策略	报告
衡量指标	愿景和目标规划	风险响应	网络安全控制	容量管理	与运营的整合	交流沟通
			脆弱性管理	记录管理		跟踪
			移动安全	问题管理		
			终端安全	危机与事件管理		
			逻辑访问控制	生产变更管理		
			软件风险控制	发布管理		
			物理访问控制	资产管理		
			环境控制	外包策略		
			数据保护	合同制定与监督		
			项目开发管理	业务持续管理组织		
			项目变更管理	业务持续管理运行		
			项目资料文档管理	备份中心管理		

运营模块

组织架构
实务和规程
工具与技术

图7.IT风险监控指标体系

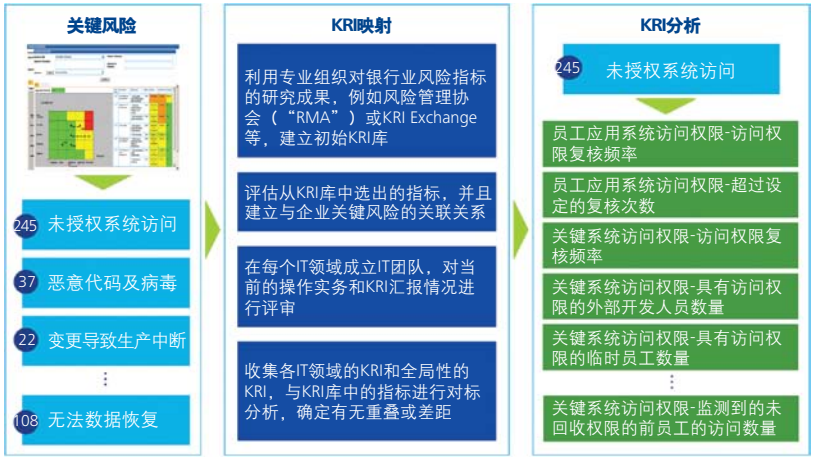


图8.IT风险监控



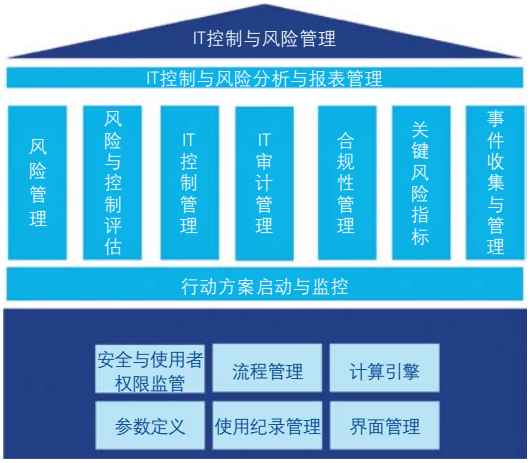
监控信息技术风险管理绩效（图7）

随着各银行内控的执行和变化，银行需要及时了解关键信息技术风险的变化趋势和状态，这就需要银行致力于关键风险指标的设计和监控。

通过建立监测关键风险变化的关键风险指标，并将关键风险指标的以仪表盘的形式展示给信息技术风险管理人员，使信息技术风险管理人员能够及时了解信息技术风险的变化趋势和现状，并及时作出响应。（见图8）

德勤一直致力于为客户推行信息技术风险管理的落地服务，借助信息技术在组织中进行风险管理流程的固化，以确保信息技术风险管理的策略和流程得到落实，使得信息技术风险管理为客户带来业务价值的最大化德勤依据国际信息科技风险管理最佳实践，设计开发了一套信息技术风险管理信息系统IT Risk Integrator，可协助银行建立以信息技术风险管理为基础的系统平台。（见图9）

图9.德勤IT Risk Integrator的系统功能架构



加强电子银行交易风险管理，提升客户安全体验

何晓明　经理
德勤北京事务所
企业风险管理服务

引言

“以客户为中心”的经营理念是银行实现服务转型和产品创新的基础，也是银行提升市场竞争力的源头，而电子银行业务不同于传统银行业务，其实际上是为商业银行等金融机构开展其他业务、销售产品与服务提供了一个电子网络平台，并可以在此基础上构成可独立存在的业务品种。而作为银行业务运行的平台，电子银行的安全性和可靠性的要求较高，风险已不仅来源于银行与客户之间的互动关系，除了传统意义上的金融风险之外，很大程度还与第三方行为有关。因此，银行在优化流程，改善服务的同时，全方位做好电子银行服务渠道的安全保障，通过针对交易过程的风险管理，持续提升电子银行服务质量、服务能力和服务水平，为客户实现差异化服务，提高客户的安全体验，是提升市场竞争力，保留并吸引优质客户的重要手段。近年来，我国电子银行相关案件频发，银行电子交易渠道也已逐步成为不法分子攻击破坏的重要目标，欺诈手段层出不穷，作案手法不断翻新，安全形势日益严峻，给商业银行业务推广和声誉带来极大的破坏力，加强电子银行业务的安全与风险管理已成为各商业银行当前迫在眉睫的任务。

电子银行业务及其发展趋势

电子银行业务是指商业银行等银行业金融机构利用面向社会公众开放的通讯通道或开放型公众网络，以及银行为特定自助服务设施或客户建立的专用网络，向客户提供的银行服务。

我国商业银行的电子银行业务发展迅速，电子银行客户数、交易额、交易量等指标快速增长。电子银行渠道在降低银行运营成本、提高服务效率、增强银行竞争力、拓宽产品销售渠道等方面发挥着越来越重要的作用，为银行和客户创造着越来越大的价值。

当前电子银行业务主要包括以下交付渠道：

- 网上银行，指利用计算机和互联网开展的银行业务，包括个人网上银行、企业网上银行等；
- 电话银行，指利用电话等声讯设备和电信网络开展的银行业务，包括个人电话银行，以及企业电话银行两类业务，涉及IVR自助语音服务和呼叫中心人工服务等服务模式；
- 手机银行，指利用移动电话和无线网络开展的银行业务；
- 自助设备，指其他利用电子服务设备和网络，由客户通过自助服务方式完成金融交易的银行业务，主要包括自动取款机、存取款一体机等。

电子渠道未来将成为银行业务交易量最大的渠道，并由服务渠道向营销渠道转型，从而实现由成本中心向利润中心的转换；未来电子银行将提供全面的、多元化的产品和功能服务，并利用互联网通过产品组合提高银行产品交叉销售率；分散渠道已不能满足客户需求，多渠道配合以提供一致的客户体验成为一种趋势，商业银行也会通过多渠道的协同实现跨渠道的产品销售；电子商务未来需求旺盛，而且目前发展迅猛，电子银行也将利用电子商务浪潮追逐新的利润增长点。

电子银行交易面临的风险

电子银行现在和将来给商业银行带来的价值毋庸置疑，其方便快捷的特性也深受广大银行客户欢迎，但电子银行通过互联网、通信网等开放性媒介运作的特点，也使得其面临诸多的交易风险，这也是电子银行为银行和客户成就更大的价值的阻碍之一。

电子银行交易风险，是一种综合性风险，包括：内/外部欺诈，指银行内、外部人员有意通过恶意使用权限或者手段进行电子银行交易欺诈；工作疏忽：因为内部管理疏忽或者内部控制力低下导致用户账户损失或缺乏阻止交易欺诈的发生的能力；信息安全风险： 外部恶意攻击或者欺诈，获取用户账户，窃取用户资金。

从电子银行交易面临的主要风险来源分析，既包括由于客户端的不当使用所造成的风险，也包括银行端由于管理或系统漏洞导致的风险。

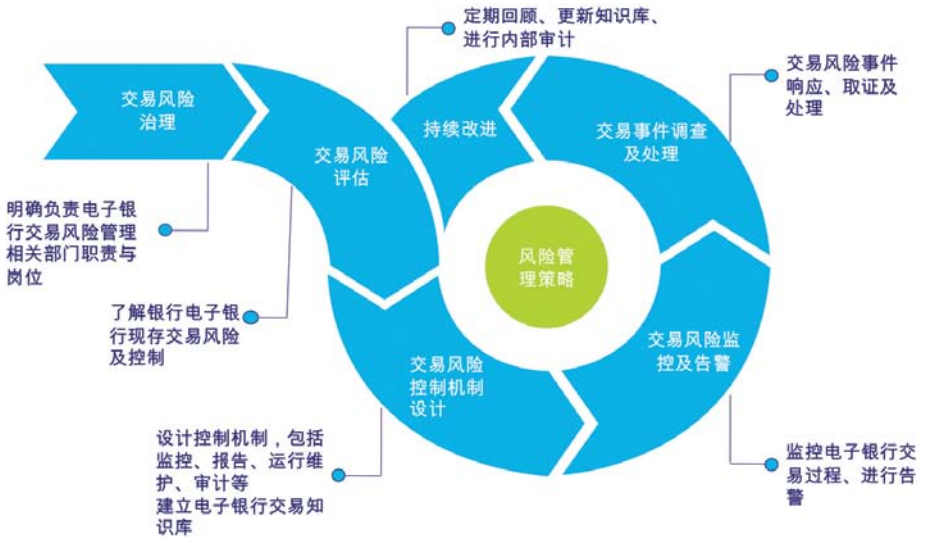
潜在风险	可能的原因
账户或身份信息丢失	• 由于客户端安全防护措施缺乏导致的帐户信息泄露 • 由于客户密码设置简单导致的帐户信息泄露 • 无意识将帐户密码泄露给第三方；
	• 业务申请时造成的客户身份信息泄露 • 系统缺陷造成的客户身份信息丢失；
非授权操作导致的资金损失	• 未经授权将资金转移至第三方 • 未经授权进行投资造成损失
客户欺诈造成银行或商户损失	• 客户拒绝承认发起的交易 • 非法分子利用漏洞进行非授权交易，造成银行或商户损失
恶意攻击导致无法正常提供服务	• 内/外部人员利用已知漏洞对系统进行攻击，造成无法正常提供服务
内部违规操作	• 业务办理人员不按规定办理业务，为舞弊行为造成可乘之机 • 关键岗位员工有预谋地互相串通，开办或进行非授权交易

而根据美国联邦金融机构检查委员会（FFIEC）对电子银行业务交易风险的描述，电子银行交易风险分为舞弊、业务操作错误和系统破坏三种类型，这三种不同类型的交易风险，对于电子银行交易发生的关键要素，包括交易目的、交易方、交易流程和交易渠道等方面，则有不同的影响和特征体现，识别这些特征并据此进行实时监控以发现潜在的交易风险并采取有效措施予以应对，是实现有效的交易风险管理，提升客户安全体验的关键。

德勤电子银行交易风险管理方法论

实现电子银行交易风险管理，应当在银行整体风险管理策略的指导下，制定对电子银行交易风险的容忍度，明确组织及职责，并通过建立日常管理流程、规程和制度，部署必要的技术手段实时监控潜在的交易风险，使交易风险监控工具始终契合业务变化及业界安全动态。德勤建议采取以下六步方法进行电子银行交易风险管理：

德勤电子银行交易风险管理方法框架



第一步，交易风险治理：

电子银行交易风险管理包括制度、规范、流程、监控工具的部署、使用及运行维护等活动。这些活动及控制机制需要有专业的组织对其负责，才能达成预期效果，并且能够确保随着业务发展，该组织可以对电子银行交易风险管理体系进行相应的变更。在此阶段银行需要确定以下问题的解决方案：

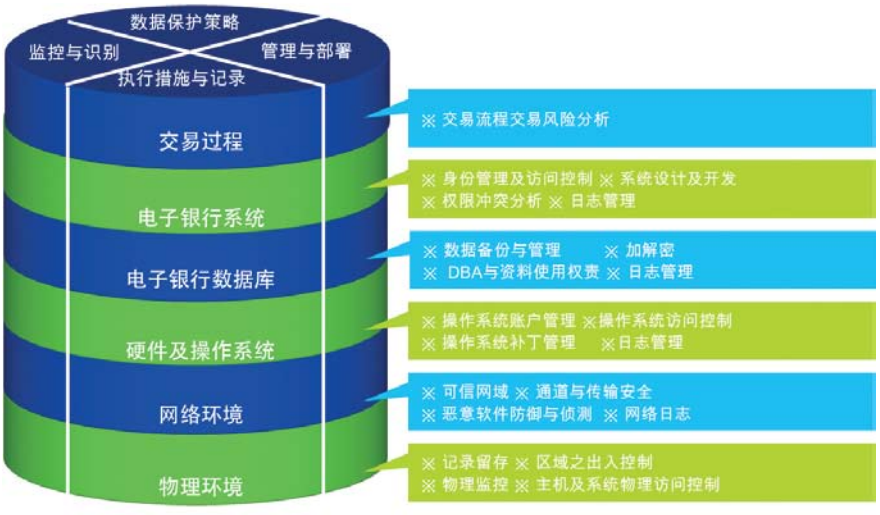
- 如何设置电子银行交易风险管理专业组织及职能？如何制定电子银行交易风险相关工作的规划、实施、推进、监控及改进机制？
- 如何确立电子银行部、信息科技部以及其他相关部门在电子银行风险管理方面的职责分工及沟通协调机制？
- 如何设定建立电子银行交易风险管理策略？
- 如何明确电子银行交易风险管理的范围、目标和工作原则？

第二步，交易风险评估：

电子银行交易风险管理应当从整体的观念出发，全面梳理现有的电子银行系统的各个组成部分，对已有的技术措施以及自动化机制进行识别，确认可以成为交易风险识别来源的关键输入，以保护现有投资，并且对后续监控系统的接入提供接口需求。在此阶段银行需要确定以下问题的解决方案：

- 如何建立电子银行交易风险评估的流程以固化交易风险的识别及评估机制？
- 如何建立对电子银行业务相关的流程、应用、系统、基础架构的风险评估和分析方法？
- 如何梳理和构建电子银行交易风险及现有控制机制的清单和框架？
- 如何识别相关交易风险特征来源，建立整合交易风险与交易要素的关联视图？

交易风险评估内容框架



第三步，交易风险控制机制设计：

电子银行交易风险管理相应制度、策略及指南，是有效管理及使用交易风险监控工具的必要因素。基于这些制度，工具的告警、应对、工具本身的账户、数据安全才能够纳入到交易风险管理体系中。同时，交易风险监控的技术手段，需要基于银行自身电子银行交易特性，首先制订出相应的策略库和知识库结构，才能最有效地使用工具。在此阶段银行需要确定以下问题的解决方案：

- 如何建立电子银行交易风险处理相关制度及规范？
- 如何建立交易风险模式库，包括攻击迹象(信号)、对应的攻击模式、对应监控点及风险阈值及对应的控制措施等？
- 如何根据交易要素设立用户行为模式特征，具体内容可能包括用户登录地点(IP地址库)、方式(UKey)、文件证书、信用卡)、通常资金余额变动额度、余额变动趋势、帐户操作模式、支付对象等？
- 如何完成交易风险监控工具的部署以及规则设置？

第四步，交易风险监控和告警：

充分利用电子银行交易风险监控工具，设置合理的规则以发挥其技术手段的作用，交易风险监控系统应当能够识别某些实时监控时显示为正常的行为，但经过时间、行为或批处理过程，表现异常的交易（例如有账户有不多的往来发生，但在某一周内，连续有多笔超出原有通常额度的交易频繁发生）；根据风险高低建立告警及升级机制，并能够关联多种信息来源，汇总并分析异常交易。在此阶段银行需要确定以下问题的解决方案：

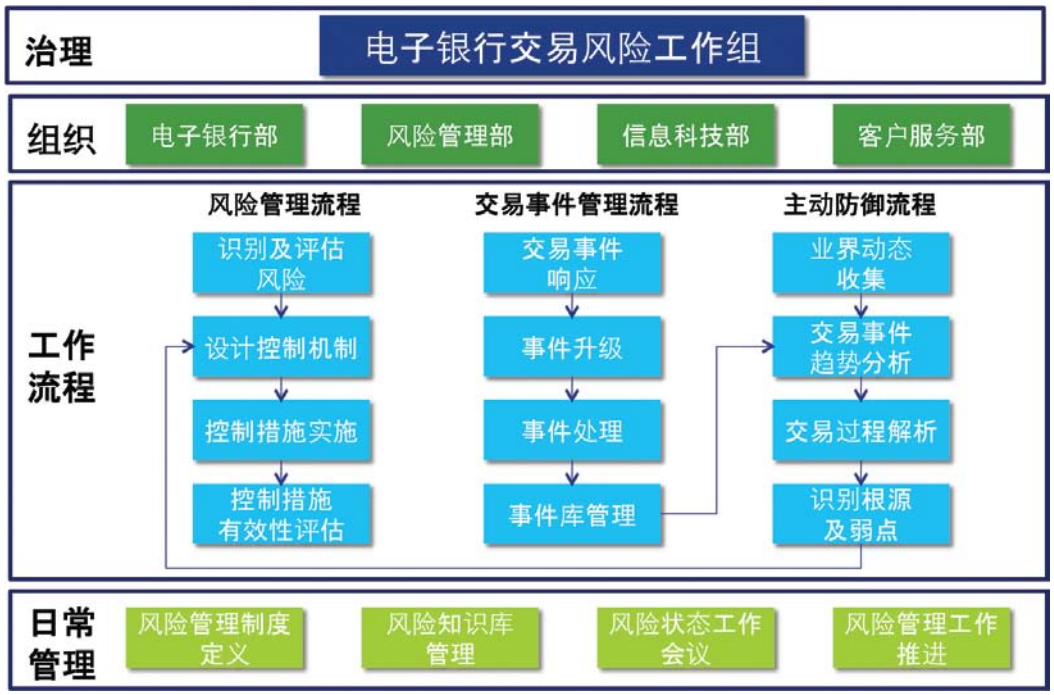
- 如何根据上阶段的用户行为模式及交易风险特征设置合理的监控规则？
- 如何定义交易风险监控及告警流程？如何建立告警升级机制？
- 如何根据用户行为模式和当前交易风险高低确定必要的控制措施，如日志记录、告警、二次交易验证或行为阻断等？
- 如何对异常交易行为进行汇总分析，识别系统化系列攻击迹象并优化监控规则？

第五步，交易事件调查和处理：

系统监控的结果需要经过人为的分析判断，才能确定应当采取的措施。例如，DDOS攻击，可能预示着有钓鱼网站欺诈；密码试探攻击，可能意味着黑客试探网站薄弱环节；应用系统多次抛出异常、日志中包括数据库访问异常、网页过滤异常字符，都预示着黑客可能在进行跨站或注入攻击等行为。银行需要根据事件迹象进行分析，是偶发攻击、意外、还是一系列攻击的开始迹象，或是在某一群体存在的共同趋势/弱点。在此阶段银行需要确定以下问题的解决方案：

- 如何建立电子银行交易事件管理流程以及事件处理和升级机制？
- 如何对客户损失进行补偿？ 如何降低银行在交易风险事件发生后导致的声誉损失？
- 银行应如何将电子银行交易事件调查与信息安全及运维管理应急响应规程衔接？

交易事件回应管理框架



第六步，持续改进：

随着业务和技术的不断发展，银行需要定期对告警、日志和出现的交易事件、包括业界安全动态进行分析，评估欺诈风险，调整应对的策略，安排专人负责汇总、分析事件迹象以判断这些迹象之间的关联，深入分析事件是偶发攻击、意外、还是一系列攻击的开始迹象，或是在某一群体存在的共同趋势/弱点，并持续地对交易风险管理策略、技术手段、应对措施等进行优化改进，保持与业务发展和技术更新的同步。在此阶段银行需要确定以下问题的解决方案：

- 如何建立定期对电子银行交易事件的分析机制，识别交易事件发生的根源，更新交易风险策略库，制订改进措施？
- 如何获取外界电子银行交易事件和安全动态并与策略更新及技术手段优化进行关联？
- 如何与内部审计部门协同工作，对制度执行及工具使用和维护的符合性和有效性进行审计？

结束语

电子银行交易风险已经得到了世界各国银行业监管机构的高度重视，中国的银行业监管机构也相继发布了《网上银行系统信息安全通用规范》、《电子银行业务管理办法》、《电子银行安全评估指引》等监管要求，用来指导国内金融机构应对电子银行安全和风险管理。

全方位做好电子银行服务渠道的安全保障，持续提升电子银行服务质量、服务能力和服务水平，是提升市场竞争力，保留并吸引优质客户的重要手段。因此，提高电子银行客户的安全服务体验，通过先进的技术与管理机制实现差异化、人性化服务，是电子银行业务发展面临的主要问题之一，也对商业银行的电子银行业务管理水平提出了新的要求和挑战。加强电子银行交易风险管理，通过先进的技术手段提升客户安全体验，协助银行强化“以客户为中心”的经营理念，也必将使银行的电子银行业务发展面临新的机遇。

Web应用安全，您再也无法忽视的风险

朱磊　副总监
程诚　副经理
德勤上海事务所
企业风险管理服务

作为近十几年全球信息化革命中最为重要的标志，互联网给现代社会带来了前所未有的变革。在这场变革中，企业与企业之间、企业与消费者之间以及消费者与消费者之间的沟通和交流正在变得越来越便利和高效。作为互联网应用的主要形式之一， Web应用无疑已是当前商业领域中无所不能的多面手，无论是通过网上商店拓展企业的销售渠道，通过电子银行提高支付的安全性和效率，还是通过内部OA系统来强化沟通效率，Web应用在各类商务应用中都已经占据了统治地位。

Web应用以浏览器为核心单一环境，与传统意义上纷繁复杂的客户端/服务器端应用相比，在开发、部署和维护上都有较为显著的成本优势。因而，无论是ERP应用，还是人事系统或银行账务处理、税务处理，Web应用都丝毫不显弱势。

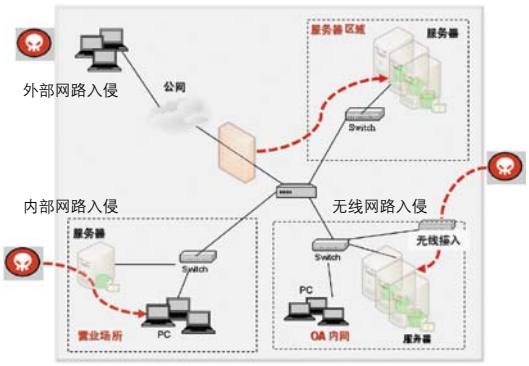
随着商务应用的普及，Web应用理所当然的成为了敏感信息流通聚集的场所，恶意攻击者正越来越多的通过攻击Web应用来获取商业机密或个人隐私等敏感信息。可以说，Web应用安全已经成为企业无法忽视的风险，也是当今信息安全风险管理的关注重点。

根据Symantec的报告[1]显示，在2009年，全球约有75%的企业曾经遭遇过网络攻击，每家公司的平均损失约为200万美元；约40%的企业表示，与自然灾害、恐怖袭击和传统犯罪相比，预防网络攻击更为重要。在所有的网络安全问题中，有80%的互联网安全漏洞发生在Web应用层面[2]。

不同于传统的IT安全工作，Web应用安全管理的难点在于企业在互联网环境之下面临着更为复杂多变的内外部环境。传统上，企业为了保障信息系统安全，通常会使用不同的技术，例如访问控制技术、防病毒技术、加密技术等等来保护各类对外/对内的应用系统的边界。但对于Web应用而言，防火墙或者其他安全措施必须开放相应的端口允许对于Web的访问，进而与服务器进行通信。此类访问可能带有恶意的企图，但通过技术手段很难进行准确的判别。

需要指出的是，攻击可能源自外部互联网，也可能来自内部人员（见图1），同时Web应用是由软件功能构成的，软件通常会包含一定缺陷(Bug)，这些Bug 就可能被恶意人员利用，实施各种恶意的操作，或者偷窃、或者操控、或者破坏 Web 应用数据、甚至利用Web系统作为攻击跳板，破坏企业的整个信息系统。

图1.入侵的可能路径



在互联网环境之下，隐蔽、利益驱使和产业化也已经成为了针对Web应用威胁的特点，大量的具备自我繁衍、自动隐藏的病毒、木马、蠕虫、钓鱼软件往往不直接影响业务的运作，而通过多次的跳板渗透入企业网络，隐蔽性地寄生在企业的服务器或终端之中，待探究到有价值的信息后再将数据传输回攻击者手中。

[1] Symantec Inc. State of Enterprise Security Report（2009年）

[2] SCMagazine. Web apps account for 80 percent of internet vulnerabilities.（2009年）。

虽然企业在IT安全上的投入上逐年增加，安全硬件软件厂商也不断的更新其产品功能以应对层出不穷的攻击破坏手法，但我们认为在未来很长一段时间中，Web应用安全作为互联网安全中的一个重要元素将是牵动无数企业神经、影响电子商务开展的巨大障碍。

在笔者近期为某移动通信运营商提供的Web应用安全评估项目中，根据客户要求，德勤对其运行在互联网上的网上营业厅及子系统、内部网账务及网管系统、以及办公网络中的12,000余台主机进行技术安全评估，并以是否能获取敏感数据为结果向企业管理层揭示风险程度。最终，笔者所带领的团队利用Web应用上的代码漏洞、访问控制及密码管理漏洞，成功地获取了分布于80多台服务器中的数百万项业务敏感信息（记录）。该评估项目在帮助客户快速解决其短期存在的安全漏洞的同时，也通过实例增强了管理层对于Web应用安全的重视，推动了其集中式信息安全中心的建立，并使得一些安全管理（如Web应用代码复核）实现了专岗化和常态化。

德勤的Web应用安全服务充分体现业务导向的理念，我们从业务目标出发，采用由上而下的方法帮助客户识别那些以WEB方式运行，包括外部互联网（Internet）及内部企业网络（Intranet），的业务应用中可能面临的各类风险，并提供防范这些风险的一站式解决方案。我们的具体服务包括：

- 利用技术手段评估安全弱点的严重程度（如网络/主机安全漏洞扫描和渗透测试），进而评估其安全管理水平；
- 设计适合客户具体应用的方法论判断在面临到不同威胁时可能产生的风险水平，覆盖策略、人员、流程及技术等各方面；
- 根据风险评估的结果，结合现有的安全管控手段提出策略、人员、流程及技术层面的改进方案；
- 为客户提供包括ISO/IEC 27001信息安全管理体系合规准备等体系咨询服务；
- 帮助客户在实施和部署改进技术方案过程中，选择厂商/产品，并在项目实施的整个生命周期中提供项目管理办公室（PMO）支持。

我们相信，WEB应用安全，是企业再也无法忽视的风险！



双管齐下 高枕无忧
—数据防泄露在行业中的应用

李 扬 经理
王婧媛 高级顾问
德勤北京事务所
企业风险管理服务

前言

保护敏感数据防止未授权泄露已经成为全球公司关注的一个重大问题。从官方统计和媒体的报道，我们看到各行业例如制造业、通信行业、金融行业、医疗行业等发生的信息泄露事件呈现出上涨态势。信息泄露的频发并不是偶然，在利益的驱动下，通过非法渠道获取有价值的商业信息来谋取更高的利润，已经形成了成熟的地下产业链条。

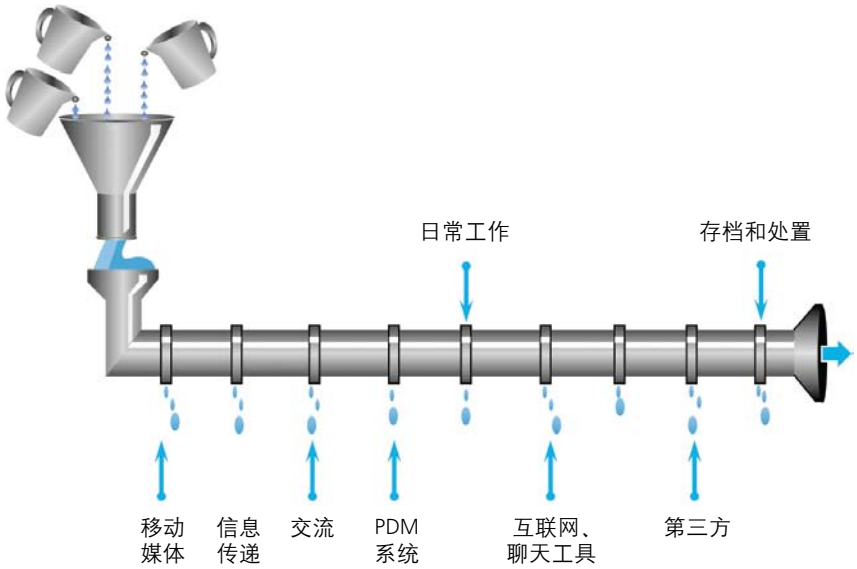
企业的核心信息对于一个企业生存、发展的重要性已不言而喻。制造业方面，尤其是涉及到产品设计和生产的企业用户，其核心数字化的设计资料直接关系到了企业的核心竞争力；通信行业方面，对客户的身份信息、私秘通讯记录的保护则是企业则无旁贷的责任；金融行业，需要在保护客户隐私同时，确保资金的安全；医疗行业方面，对于病患隐私信息的保密的监管要求也越来越强势。以上的例子，仅仅是在信息经济时代，企业核心信息资产的冰山一角。任何一个行业中的任何一个企业都无法承受数据泄露带来的生产停工、生产力下降、数据丢失、滞销以及企业声誉受损等影响。

数据防泄露安全形势

为何在企业日益重视安全技术的情况下，信息丢失事件仍会愈演愈烈呢？原因在于，一方面，随着技术的发展，企业的业务流程及信息处理越来越依赖于IT设施，企业的信息从最开始的以纸介质为保存媒体，逐渐转变为纸介质和电子介质保存的局面。许多企业出于快速处理信息的考虑，甚至将所有的信息进行电子化，所有的业务流程也依赖于IT设施。因此，当今信息应用环境的复杂度和广度都增加了企业信息的保护难度；另一个面，公共信息丢失事件带来的恐慌也让许多企业急于求成，在没有准确把握症结所在的前提前，匆匆购买技术加以实施，导致的只是事倍功半的效果。企业在执行业务活动的过程中，会存在多种信息泄露的途径，也是造成敏感资料难以保护的重要原因（见图1）：

企业很多机密资料，保存在个人电脑、文件服务器的共享目录，以及应用系统数据库，或者移动介质，也会通过邮件、即时通讯软件(例如QQ/MSN/GTalk等)。部分资料由于工作原因，需要外发至供应商、分/子公司或者客户。在这一过程中，有各种环节可能会导致这些机密资料被泄露或者被修改。

图1.数据泄露途径



通常在企业内，存在如下现状，成为了对关键信息进行保护的重大挑战（见表1）：

很多企业对信息安全，特别是对关键信息的保护，存在管理方面的一些误区，导致从表面上看，有了充分的技术手段进行防护。但从风险角度进行评估，实际上还存在较为严重的安全隐患。

误区一：保护关键信息的主要方式应该是使用加密；

如果不能清楚地识别需要保护什么，就不可能真正管理好。而任何技术手段要真正起到效果，必须要基于管理策略和管理流程之下。加密的方式使用起来较为简单，但是由于缺乏信息安全管理的策略，使得对资料的加密难以进行控制。企业通常会采取内部所有资料都加密，外发资料都解密的方式进行管控。实际上起不到真正的防泄漏效果。

表1.

控制领域	安全隐患
信息资产管理	• 并没有对需要保护的资料进行识别，没有对需要保护的资料设置保密级别，以及对应保密级别的访问控制和信息交换策略； • 往往具备有数据备份的设备和定期备份机制，但缺乏数据恢复演练。此外，备份往往仅考虑数据自身的备份，对于数据应用的环境，包括硬件、操作系统、数据库系统以及应用系统，缺乏应用系统级的备份和恢复演练机制。
逻辑访问控制及权限管理	• 缺乏对资料外发的明确权限和权限的申请及授予方式规定； • 为平衡工作效率和安全，通常对工作环境和应用系统的账号和权限管理较为宽松； • 个人和手提电脑都有管理员权限，较难管控。
网络访问控制	• 经常存在在家办公，或者出差期间通过远程办公方式连接到公司的内部网络的情况。对于该访问权限的申请、授予、特别是权限的清理，缺乏制度化的机制定期审计和清理； • 没有根据信息的分级和访问范围划分网段，并且在不同安全等级的网络之间进行逻辑访问控制； • 公司内部未控制无线网络的访问，可以同时通过无线方式连接互联网，以及网线连接公司内网的情况。由于个人电脑的防护较为薄弱，存在通过无线互联网渗透到公司内网的安全威胁； • 在公司范围内的内网接口，没有管控，可以直接有外部人员连接网线就可以接入内网。
个人电脑及移动介质	• 普遍使用手提电脑，很难进行管理； • U盘大量在公司内部使用，缺乏管控机制。

误区二：不需要识别关键信息，对所有资料都进行加密，就能够保证资料安全；

这一误区造成的后果，被称为“加密泛滥”。基于加密机制的文档保护系统的技术局限性，会造成如下风险：

1. 主密钥被破坏(例如主密钥服务器崩溃)，会导致加密后的资料无法被解密，造成真正的灾难；
2. 主密钥丢失，所有被加密的文档都可以被解密；
3. 往往公司内部加密资料还是可以被任意访问，文档虽然不容易被传出，但是重要的信息还是可以被人员获取和泄漏。

众所周知，信息安全是一个木桶理论，任何一块短板都可能导致功亏一篑。有效的缓解信息泄露给企业带来的风险，不是单一部署某种安全产品或采用单项管理手段就可以解决的问题。德勤通过对不同行业的防信息泄露解决案例的成功经验积累，已形成了一整套体系化的解决方案。

防信息泄漏保护的总体框架

通常对关键信息的信息安全管理策略应当遵循如下原则：

1. 循序渐进，把握不断调整，不能一步到位的原则
2. 明确定义研发资料安全管控的目标，以及对应的总体安全策略定义清楚做到什么级别的安全，给一个总的策略；
3. 建立切实可行，以及对管控粒度进行平衡的信息资产分级制度；
4. 基于资产分级制度，根据级别优先管控高安全等级的信息资产，包括访问控制、信息交换、区域划分、权限和身份管理等机制；
5. 设计敏感资料的职责区隔机制，通过职责分离确保不会把各种资料都汇总到一个人手里；
6. 对于信息泄露途径进行风险评估后，基于评估结果考虑总体的管控措施。

关键信息保护，应当基于企业关键信息产生、使用、保存、传输的业务流程，从治理、运作、技术等方面，设计必要的管理和技术措施。

下面是防信息泄漏保护方案的总体思路（图2）：

首先，明确信息资产

必须要先明确管理对象是什么。因此要对信息资产首先进行识别和管理。信息是一种资产并且是无形的，包含了大量的业务数据、客户信息、商业秘密等内容，所以首先要对信息进行全面的梳理，了解现有的需要进行保护的信息内容以及对信息进行处理的系统环境。在此基础上，需要基于信息对业务的重要程度，对信息资产进行分级。这一级别代表了对信息资产如何进行访问、如何进行传输，以及信息安全风险可能造成的危害程度。

其次，在对信息资产分类分级整体策略基础上，考虑对于信息生命周期各个环节的安全措施。

如图3所示，通常情况下，对于核心信息的保护，需要从信息的获取、保存、使用、共享、归档、处置等各个阶段，综合考虑需要采取的安全管理或技术措施，同时，基于信息价值的角度，审视各个环节的安全防护措施，是否会导致散落信息整合后，导致对公司有损害的信息泄露事件。具体措施的采取则应包括管理流程、应用系统、数据库、操作系统平台、网络环境以及物理环境等方面。一般在基于对企业现状了解的基础上，在建议具体措施选择过程中会把握以下主要原则：

- **适度原则**：安全措施的选择应当考虑投入产出比，以有限的资源实现对于最重要信息的重点保护，兼顾对工作效率的影响以实现最佳防护效果，而不是一味追求全面最优的配置；
- **渐进原则**：安全措施应充分考虑预测当前管理和技术成熟度，循序渐进，逐步建设全面的安全防护措施；
- **全面原则**：兼顾管理与技术两方面的措施，在确定对于研发技术信息安全管理要求的基础上，充分利用技术手段，实现全面的安全防护，取得最佳效果。

图2.敏感信息保护路图



图3

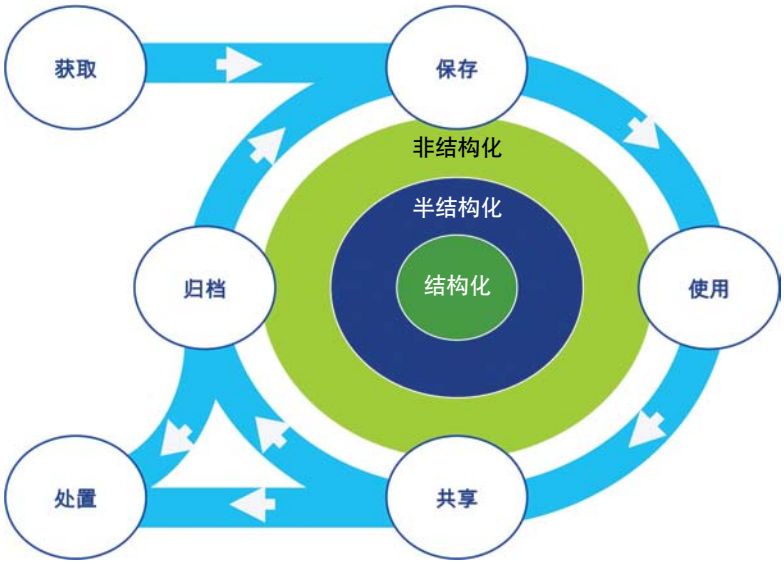


图4.IT风险管理方法论

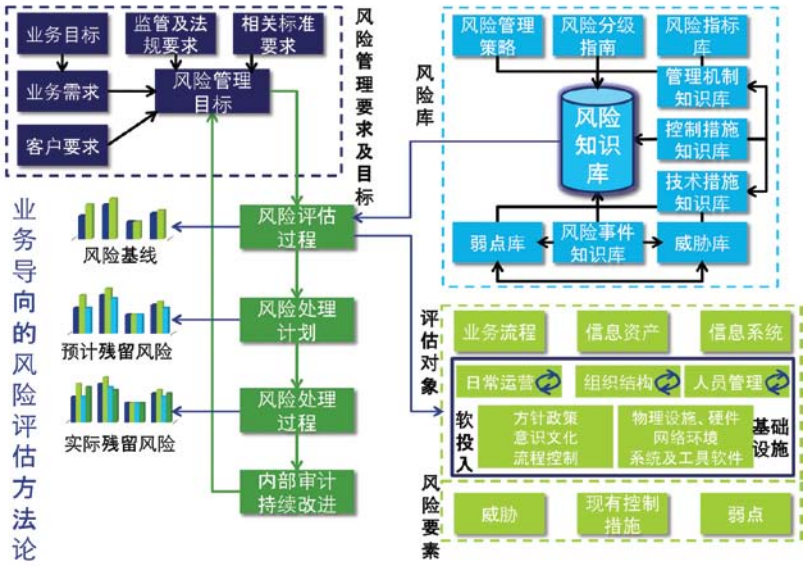
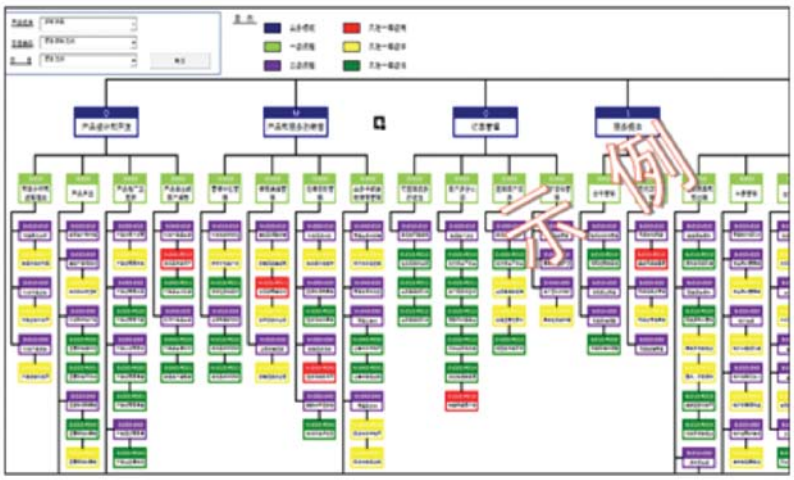


图5.基于业务的信息安全风险全貌



第三，识别信息资产生命周期的基础上，识别造成信息资产被泄露或者被篡改、破坏的信息安全风险

德勤开发有业界领先的风险评估方法论。方法论根据不同的行业特性建立风险评估原则，包括风险评估所参照的评估依据和准则，从而保证了风险评估的充分性和完整性。方法论将评估对象分为服务、业务、流程、信息资产四个层面；在管理的角度，包括了治理、组织、政策、运营等方面；风险对象分为威胁、弱点、控制措施。评估方法和评估过程应用德勤自身独有的行业业务知识库(Industry Print)以及风险知识库(RACK)，从业务、流程及信息资产三个层面对IT业务进行评估。这一德勤所独有的风险评估方法论，针对于客户核心业务，通过多层次多维度对业务进行评估，能够从总体业务、核心流程以及关键信息资产等方面，展现最为全面的对合规要求及业务要求的满足程度，并且更有利于开发出更为全面的风险处理计划，从而更有有效地消减所发现的风险。信息安全风险评估方法论如图4所示：

通过信息安全风险评估，德勤协助组织揭示在业务过程中信息资产存在的信息安全风险全貌，使组织可以基于风险对业务造成的影响开发更有针对性地信息安全规划和风险处理计划（见图5）：

第四，在多层面应用安全控制措施，对可能造成信息泄露的渠道进行防范 。

在识别敏感信息在业务环境中的生命周期基础上，德勤基于自身的敏感信息保护风险知识库，识别业务过程中的敏感信息风险热点，并在建立资产分级以及基于分级的访问控制策略基础之上，建立职责区隔机制，并且应用德勤敏感信息保护信息安全框架(ISF – Information Security Framework)，在六个层面，四种视角共24个控制领域，贯穿敏感信息生命周期的各层面以及工作流程上，进行全方位的安全管控，确保在使用中(Data in Use)、存储中(Data at Rest)、传输中(Data in Motion)的敏感信息均得到充分的保护。并通过安全审计及监控，使敏感信息的授权使用、权限管理等活动，均在控制当中。当出现风险迹象时，能够被及时识别并且采取相应控制措施规避风险。

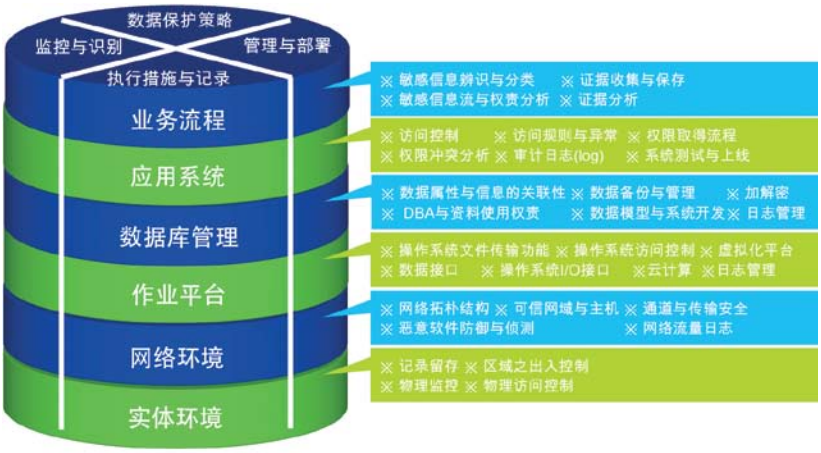
最后，对有针对性地安全防范措施进行实施

对于所确定的安全防范措施，管理上的内容形成具体的安全制度规范，技术上的要求则通过实施相应的工具，或对系统配置的优化加固进行落实。典型的管理措施包括研发技术信息的具体分类分级的制度，在此基础上制订的访问控制要求，为实现访问控制而制订的安全域划分的原则，安全域之间以及安全域内部信息交换的规范，技术措施则包括但不限于终端机器的访问控制（如USB端口、屏幕保护、口令策略等）、网络流量监控、关键服务器的隔离、物理访问控制以及一些DLP的专用工具的部署等。

基于数据防泄漏的方法论(Data Loss Prevent – DLP)，是区别于传统的加密方法的关键信息保护的体系化框架。通过建立安全策略、管控机制、结合管理规程与技术手段，结合信息生命周期管理及有限加密原则，切实缓解关键信息泄漏的风险。数据防泄漏方法论能够帮助企业达成以下效益：

- 明确组织内信息安全的总体管理职责，以及各部门的安全职责；
- 识别组织内关键信息资产，对资产进行分级，并且明确信息资产的所有者、保管者和使用者的职责；

图6.敏感信息保护相关控制



- 根据信息资产级别，制订信息资产的生命周期安全管理策略以及访问控制方针。即，明确谁、什么时候、通过什么方式才能获取访问或者传输资料的权限；访问权限与信息资产的保密等级、人员的工作职责相关联；访问、使用和传输过程被监控和审计等。
- 协助组织进行基于信息资产的信息安全风险评估，基于风险优先级建立数据防泄漏体系建设规划；
- 部署数据防泄漏(DLP)工具，结合有限加密的策略和加密工具，对信息资产的生命周期进行管理，对信息资产传输至U盘等可移动介质、或者上传至网站或邮件发送、批量复制资料等行为，基于所制定的访问控制策略进行监控和阻断。结合对于最关键信息的加密，形成全方位的保护。
- 建立信息安全事故处理流程，建立快速响应和处理信息安全事故的机制；
- 建立信息安全审计机制，包括审计职能、培养审计技能，以确保对安全控制措施的切实执行。

新环境下的企业信息系统日志分析

李逸元 副总监
德勤上海事务所
企业风险管理服务

本文首先介绍了在新的企业发展背景条件下计算机系统日志分析和审核的现状和重要性；在讨论了日志的分类和针对不同功能系统的日志分析要点后，我们也介绍了近两年业内关注的Splunk日志分析技术方案。为企业在日常工作中通过日志获取和分析来对信息安全进行监控提供了参考和指引。

关键词：信息系统安全，日志分析，计算机审计，Splunk

前言

近年来伴随着电子信息产业的飞速发展， 新的电子信息技术层出不穷。新的技术也在推动全球的企业进行变革。可以说，任何一家企业想做大做好， 都不得不依赖于信息技术， 而新的技术给企业带来无限机遇的同时，也带来了巨大的挑战。反观近年来发生的各种电脑舞弊案，数量呈增长趋势，手段花样翻新，防范难度越来越大，给企业带来的损失也越来越大。

在这样一个背景下，信息系统反舞弊这一新兴的课题，得到了越来越广泛的关注。 全球很多国家和组织都颁布了针对信息系统的管理规范， 例如ISO20000和ISO27001/ 27005。 中国国内也颁布了相应的国家标准， 并针对金融等高风险行业制定了针对行业的信息安全准则。通过深入的研究，我们不难发现， 现有的计算机反舞弊方法主要分为两类: 第一类是控制，例如采用密码，加密等技术， 在系统上强制实施职责分离等。第二类是监查， 主要的手段就是通过记录分析系统的运行情况特征和产生的轨迹，通过对这些轨迹的分析和研究，来判断是否产生了舞弊。这些系统的轨迹我们通常称之为日志， 而这正是本文要讨论的内容。

日志的定义与分类

日志就是系统对某些对象进行的某些操作和其操作结果，比如用户登录或者是其在系统上的行为按时间有序的集合。每一个日志文件由很多的事件记录组成。每条日志记录存储着一次单独的事件。在某些情况下系统日志是一些简单的文本文件，可以被用户直接阅读。记录中主要包含了一个时间戳和一个消息。

从日志的产生来源上可以将日志分为：操作系统日志、应用系统日志、数据库系统日志、网络设备及应用服务日志等。前三种又可称为系统日志， 由系统自动生成，与系统行为密切相关。操作系统日志记录系统进程和设备驱动程序的活动。它审核的系统事件包括启动失败的设备驱动程序、硬件错误、重复的IP地址，以及服务的启动、暂停和停止。系统日志包含由系统组件记录的事情。例如，在系统日志中记录启动期间要加载的驱动程序或其他系统组件的故障，比如启动时某个驱动程序加载失败等。应用系统日志主要记录用户程序和商业通用应用程序的运行方面的错误活动，它审核的应用程序事件包括所有错误或应用程序需要报告的信息。比如失败登录的次数、硬盘使用的情况和其它重要的指针等。 数据库系统日志则记录了数据库中数据和数据结构的变化以及用户对数据的增加、 删除 、以及修改等。 网络设备及应用服务日志则主要偏重于网络设备的使用和网络服务如WWW、 FTP以及防火墙的日志，它是网络活动的缩影。

日志的审计与分析

日志的审计与分析包含两个重要的步骤：收集和审核分析。首先企业应根据自身的特点和需要对不同种类的日志进行收集和保存。 由于不同行业有不同的特点，应用系统的重要程度也有区分，管理层和信息安全人员应预先讨论并制定日志的收集方法。在收集阶段之后的保存也很重要，企业可以通过备份，逻辑控制以及采用一次性读写介质保证日志的完整性和可用性，防止日志被篡改。 完成了日志的收集保存只是工作的开始，针对日志进行分析和审核，从而达到监控的效果和质量，这才是重中之重。 企业应有明文的日志审核策略以及相应的问题处理流程，从而做到有“志”可依，有“志”必依。

目前日志收集和分析主要是针对不同系统层面以及作业流程的，再各流程又各有特点，形成一套完整的体系。

1.操作系统层面

操作系统是控制和管理计算机硬件和软件资源、合理地组织计算机的工作流程以及方便用户使用的程序的集合，故其安全性成为计算机审计安全的一项重要内容。目前，常见的操作系统有Windows、UNIX、Linux等，在进行操作系统安全审计过程中，审计数据轨迹表现为日志文件。日志文件是操作系统中一类特殊的文件，它们是计算机审计线索和证据的重要来源，记录着计算机系统发生的一切活动情况，包括系统各项服务的细节。日志可以监控系统资源，寻找可疑行为，确认入侵范围。审计人员通过分析日志文件可以了解计算机系统使用情况和安全状况，分析来自内部威胁和外部攻击的可能性等，并快速地对潜在的系统入侵做出记录和预测。例如，Windows操作系统自带安全机制，其中包含审核策略，是用来指定要记录的事件类型的，这些类型涉及从系统范围的事件(例如用户登录)到指定事件(例如某用户试图读取某个特定文件)，这些事件包括成功事件、不成功事件或兼而有之，审核记录写入计算机的安全日志，即形成电子数据轨迹，审计人员可以充分利用日志文件分析系统的安全状况，合理评价系统内部控制的有效性。

2.计算机应用系统和数据库层面

计算机应用系统是个较为宽泛的概念，它包括电子数据处理系统 (EDP)、管理信息系统(MIS)、以及作为各种服务应用的专用信息系统，它涉及对数据的输入管理、处理、存储、保护、传输和输出等多个过程，每个过程对数据的操作都会有所记录，所有电子数据均有迹可寻。

在数据输入过程中，电子数据轨迹表现为上机日志，即操作员在进行数据输入时都有上机记录，每个系统随时对不同模块或产品的每个操作员的上机时间、数据输入、下机时间等情况进行登记，形成数据输入日志。通过查阅数据输入日志，审计人员可以了解计算机应用系统的输入控制情况，包括输入数据正确性控制、完整性控制和输入错误纠正控制等。对于通过检查上述数据输入时的电子数据轨迹，审计人员能够清楚理解数据输人的过程，同时判断数据输入控制的有效性和完整性。

数据输入信息系统后，系统要对电子数据进行加工处理，系统通过相应的计算公式生成处理后的数据， 对丢失数据、重复或出错数据的处理。电子数据处理的每一个环节，系统一般都设置操作日志，自动记录所有执行过的操作，其中包括操作员信息、各个用户终端的辨认、操作时间、所调用的功能模块等。审计人员根据电子数据轨迹存在方式的操作日志，就能即时了解数据流向，检查计算机系统中数据处理系统各个环节的控制措施，进而实施有效的控制。经过初步处理的电子数据在数据库中要进行集中管理和进一步处理。

数据库是计算机信息系统中最重要的组成部分，信息系统中大多数和信息有关的操作都与数据库有关。在数据库中，电子数字轨迹表现形式是用于描述所管理的表和对象的数据，即数据字典，是关于数据的数据，也称为“元数据”。数据字典存储有关数据库结构信息的一些数据库对象，它描述了实际数据是如何组织的。一般情况下，数字字典包括表或视图的一般信息 (如表名，别名和描述等)、数字定义 (包括数据类型，数据长度和结构组成)、数据的使用特点 (包括数据的取值范围、使用频率和使用方式)、数据的控制信息 (包括数据来源、用户、使用它的程序和改变)等主要内容。审计人员可以通过分析各种数据库表以及视图之间的关系，并选择出与核心业务处理直接关联的数据库表和视图，对表的结构，包括字段类型、取值、空值应用、各种编码的含义、有效性和一致性进行详细分析研究，找出属于系统内控有关的关键字段。然后通过相关数据库表之间关联，找出规律性的数据记录，发现疑点和审计线索。

触发器是一种特殊的存储过程，由数字字典创建和指定的，它在插入、删除或修改特定表或视图中的数据时触发执行，它比数据库本身标准的功能有更精细和更复杂的数据控制能力。触发器可以跟踪用户对数据库的操作，如审计用户操作数据库时所调用的语句和把用户对数据库的更新写入审计表等；触发器还可以基于数据库的值使用户具有操作数据库的某种权利，可以实现复杂的数据完整性规则，可以实现复杂的非标准的数据库相关完整性规则。触发器可以对数据库中相关的表进行连环更新、同步实时地复制表中的数据、自动计算数据值等作用。审计人员可以利用触发器技术实现对电子数据的跟踪和保护。

另外在一般的大型数据库中都存在用于捕捉系统活动的工具，如Microsoft SQL Server中，SQL Serve Profile工具就是用来捕捉系统的活动，用于SQL跟踪的图形用户界面，用来监视Microsoft数据库引擎或Analysis Services的实例。这些工具可以捕获每个数据库事件的数据，并将其保存到文件或表供以后分析。例如，可以用于监

视产品环境，以了解哪些存储过程执行速度太慢并妨碍性能。审计人员可以先创建一个跟踪定义，然后就可以启动和运行跟踪，监测相关服务器上的SQL server事件，并且为所选的事件捕捉满足过滤条件的指定数据。Oracle数据库从其安全性考虑，设有多个安全层，并且可以对各层进行审计。可以被审计的三种不同的操作类型包括注册企图、对象访问和数据库操作。利用其中对对象的数据交换操作审计功能，就可以获得相应的电子数据轨迹。因此，充分利用数据处理阶段产生的电子数据轨迹，可以有效分析和判断数据处理控制情况，包括处理权限控制、业务时序控制、合理性检验控制、参照检查控制和审计踪迹控制以及恢复和备份控制等。

最后一个阶段是数据输出，计算机信息系统的输出如果出错或者输出数据未经允许被窃取或使用，都将可能给企业带来损失，故必须进行输出控制。实现输出控制措施有：只有经过授权的人才能下载数据，并进行操作登记；进行输出条件的检查、输出完整性和正确性检查、输出数据的安全保护、输出格式的控制等。通过了解系统输出控制措施的设置，就能清楚输出过程中电子数据轨迹的表现形式。

3.网络应用层面

网络应用方面通常记录的信息有时间戳、基本的IP特征：如源和目标地址、源和目标端口和IP协议 (TCP、UDP，ICMP)、匹配流量的规则号、执行的动作：如接受、丢弃或者拒绝连接，以及描述性文本解释。维护人员可以通过它来分析网络服务的情况，检查错误发生的原因，快速定位故障，保障网络可靠运行；监控用户的使用行为，综合审计网络信息，保障网络安全可靠。在监控性能的同时，还可以根据日志记录下来的信息发现异常情况或者受到攻击时攻击者留下的痕迹，从而加强网络安全等级，提高网络安全系数。

日志分析工具

很多系统都自带了简单的日志筛选分析工具，如Windows系统自带的日志查看器。 这些工具在日常工作中帮助企业收集，分析日志，从而达到监控的目的。但是随着信息科技的发展，传统简单的日志分析工具受到了极大地挑战。首先IT硬件环境平台百花齐放，同一功能类型的产品会有多种品牌多个系列，因此当一个中大型组织和机构面对如此众多但又必不可少的IT设备时，对于IT的网管人员管理的难度是可想而知，他们迫切需要一个综合的数据平台，能够统一查看这些设备的状态，而不需要每天都到设备上登录一次；需要一个能当这些设备出问题时，快速定位出问题所在的机制；需要一个能快速生成报表，并且能够整合多台设备数据生产报表的系统。其次， 组织和机构为了信息化建设，将会开发各种IT业务系统，旨在提升工作效率，减少繁复的工作流程，整合组织和机构各种资源，最终提升整个组织和机构的生产力，为组织和机构带来效益。但是随着信息化建设的不断扩大，这些业务系统也逐渐变多、变大。例如：组织和机构会有OA系统，ERP系统，CRM系统，邮件系统，财务系统，公文审批系统，组织和机构门户网站等等。同样这些IT业务系统会产生大量的IT数据，而这些IT数据又是非常重要的，因为其关系组织和机构各个业务流程的具体运营状态，如果一个系统出现问题将有可能导致整个组织和机构停摆。而这些需求如果仅仅靠现有的工具来实现，简直比登天还难。最后组织和机构开发的这些业务系统的支撑软件产生的各种IT数据，例如BEA，SAP，Vmware，Exchange，Websphere这些软件等等。对于一个中大型组织和机构拥有这么多类型软件并不是一件什么新鲜事情。但是对于系统维护人员，或者网管人员来说可以算是一种灾难，因为这些软件都是个组织和机构各种业务息息相关的，任何一个软件出现问题，都会导致组织和机构的某一个业务系统停顿，对组织和机构正常运行产生负面影响，给组织和机构带来各种损失。

因此，对于这些软件产生的IT数据，组织和机构需要一个综合的数据管理平台，能够利用这些软件的数据进行相关性的分析，能够在这些软件出现问题时最快速找到问题，能够定时的为这些软件产生运行状态报表，能够通过分析这些数据为组织和机构的领导进行信息化建设时提供数据支持。这也就造就了专业的面向多平台多系统拥有更强大功能和更新的设计理念的专业企业资源搜索软件的产生。 在此我们介绍下业内受到许多单位关注的Splunk软件。

Splunk方案介绍

Splunk是一个设计给组织和机构使用的IT搜索引擎，它利用了雅虎、Google的搜寻技术与理念，使得组织和机构可以用来管理复杂的 IT 系统。Splunk的软件能自动收集由各种服务器、网络设备和软件产生的数据与日志，其设计与使用概念就像是Google谷歌搜索引擎一样，组织和

机构一旦安装Splunk的IT 搜索引擎之后，IT人员就可以透过浏览器使用Splunk并对组织和机构的各种数据进行关键词搜寻，快速地得到所需要的数据。除此之外Splunk本身还具有计算能力，管理者可以透过Splunk将搜寻所得的结果立即做运算处理，产生各种报告、图表与警示，而且还可以设定Splunk进行排程定时搜寻，并将结果以邮件方式通知相关人员。

Splunk 是一个可运行于各种平台的 IT 数据、日志分析软件，支持的作业平台包含Windows，Linux， Solaris， FreeBSD， AIX， MacOS，HP-UX。与 Google Analytics 这一类的 Web 日志分析软件的不同之处在于，Splunk 可以支持多种 IT 设备（服务器、网络设备、应用程序、数据库等）所产生的日志，其对日志进行处理的方式是进行索引之后让管理员可以对日志中出现的各种情况进行搜索，并且通过图形化的方式展现出来。

每天由各种服务器所产生的日志的数量是非常惊人的，而遇到突发情况时，却往往能够从这些海量日志中找到最多的有用消息。通常在 Unix 下对日志进行查找使用的是 grep 之类的低效率的方式，而 Splunk 使用了现代搜索引擎技术对日志进行搜索，同时提供了一个非常强大的 AJAX 式的界面展现日志。

Splunk包含六大功能：Index（索引）、Search（搜索）、Alert（警报通知）、Report（报告）、Share（资源共享）、Secure（安全功能）

1. Index（索引）

IT人员往往在管理 IT数据时会面临因厂商数据格式变更，与老旧设备、应用程序因稽核需求而必须产出分析报告，现有的 日志管理程序无法立即支持或无法辨识。Splunk 具备比较多样且弹性的数据搜集方法，可以检索各种型态的数据，不严格限定 其格式，并收集来自多种不同的应用系统和网络设备。Splunk能够进一步监控文件系统中设定配置的变更，做变更管理，更可链接各种网络通讯端口去接收Syslog、SNMP和来自其他各式各样网络装置的数据。

2. Search（搜索）

Splunk具备自定的各种型态搜寻，而不是只有固定几种的字段，不需要指定数据的格式，更可结合时间与关键词进行搜寻，呈现出清楚的搜寻结果，使用上就像Google一样的直观易用。

3. Alert(警报通知)

Splunk能够定期排程执行，并依据搜寻结果发出各项警示通知，可以透过email、RSS或SNMP等方式链接其他管理接口，可触发执行自行定义的因应方式，例如重新启动应用程序、系统或网络设备。

4. Report（报告）

Splunk提供丰富的报表能力，能够将搜寻结果以图表呈现，更可弹性化地产制出组织和机构管理阶层所想要的报告内容。

5. Share（资源共享）

由各种设备所产生的日志数据是相当枯燥乏味的，透过Splunk可将它转化为切实可用的重要IT信息，并且能为任何人所用，不需要太多艰深的知识即可找出想要的信息。

6. Secure（安全功能）

组织和机构的IT信息其重要性不言可喻，Splunk可整合组织和机构既有的认证系统进行安全管控，确保数据在存取、分析和稽核时不会破坏数据的完整性。

总结

在企业飞速发展的大潮中，信息系统起到了巨大的作用。 因此，针对信息系统安全的问题也得到了越来越广泛的关注。 虽然只是简简单单的记录系统操作轨迹的日志，却能真真切切地帮助企业管理业务错误和舞弊。 新的理念和技术，为信息系统安全的管理提供了无限的可能，为企业创造巨大的价值。

参考文献：

- 主机日志分析与研究，李燕南，刘新，蒋伟宏，赵群，出自《中国高新技术企业》2010年第4期， 总139期，193-194页
- 基于日志分析的网络管理与安全审计系统，张俊林，出自《信息科学》2009年，671期， 42,62页
- 日志审计系统设计与实现，黄艺海，胡君，出自《计算机工程》第32卷22期，2006年11月， 67,68,93页
- 日志分析在计算机取证中的应用，王彩玲，出自《福建电脑》2006年第7期，164,169页
- Splunk方案应用技术白皮书 www.splunk.com

自动化风险管理（Automated Risk Management）—让企业武装起来

赵文华　合伙人
曾　春　经理
德勤上海事务所
企业风险管理服务

近来年，越来越多的资本市场和政府监管机构对企业的风险管理及内部控制提出了更高的要求，如美国2002年出台的萨班斯法案、全球金融市场的巴塞尔新协议、中国财政部等五部委2008年出台的《企业内部控制基本规范》，中国国资委2007年出台的《中央企业全面风险管理指引》以及中国银监会2009年发布的《商业银行信息科技风险管理指引》等。这些监管规定在极大程度上推进了全球各行业的优秀企业的风险控制能力，提升了这些企业的股东价值和可持续发展能力。毫无疑问，这些发展和进步离不开企业内部审计和风险管理职能的有效支持。然后，如何使得企业的风险管理和内部控制能更有效且高效地运作？企业自动化风险管理正是在这样的背景下应运而生的。

所谓自动化风险管理是指基于固化的，常态化的风险管理和内部控制的工作流程，通过IT技术和信息化手段，将这些工作流程自动化，从而提高企业风险管理和内部控制工作的效果和效率，最终提升企业的股东价值和可持续发展能力。

自动化风险管理的价值所在

按照摩尔定律，微处理器的性能每18个月会提高一倍，从1946年发明计算机，1990年发明互联网到现在，信息技术已经经历了无数个“摩尔周期”，在云计算，SAAS初露端倪的今天，信息技术的作用已经逐渐从单纯的业务支撑走向与全面的企业管控，所谓“工欲善其事，必先利其器”，信息技术为提高风险管理和内部控制的效率和效果提供了有利条件。接下来，让我们从及时性、透明性、有效性和成本优化四个角度来理解自动化风险管理模式的价值所在。

第一，从及时性的角度：自动化风险管理模式的高频率，高效率特点能保证企业实时进行检查，及时发现风险管理和内部控制的薄弱点：

更高的控制频率：企业可以以更高的频率进行内控检查，比如实时分析系统权限的分配是否合理。

更高的控制效率：自动化风险管理模式使得内部控制检查的结果更加精确和更具针对性。企业人员可以通过内控报表即时获得企业的风险管理现状，从而有的放矢地安排整改资源。

及时发现风险，增强管理能力：自动化风险管理能够建立实时的风险预警机制，使得企业可以对特定的风险指标进行实时监控。比如，企业可以迅速识别职责设置时的冲突情况，比如凭证的录入和凭证的审核职责不能同时授予给同一个人，针对这些冲突，平台可以自动预警。

图1. 自动化风险管理的价值图示



第二，从透明化的角度：自动化风险管理模式应用了信息化平台进行权限配置以及数据管理，降低了人为僭越舞弊的可能性，也提高了各类数据应用的有效性和透明度：

减少舞弊：企业可以即时监控特定的控制活动，从而减少舞弊的发生。比如即时生成采购订单报表，列示所有采购订单创建人和审批人相关的情况。

更多更便捷的管控报告：企业可以根据需要随时获得各种类型、维度的风险管控报表，从而对企业的风险管理现状有更好的认识。

第三，从有效性的角度：自动化风险管理模式将风险管理和内部控制的流程通过信息化手段体现，能够做到所有流程的标准化，降低差错率：

提高管控标准化：自动化风险管理使得企业能够建立和实施统一标准的内控检查体系，从而提高内控检查的质量。

更低的差错率：自动化风险管理模式较常规的手工内控检查避免了人为的操作错误。同时，企业人员可以不再采用抽样测试而是采用全盘检查的方法，从而使得内控检查无遗漏。

第四，从优化成本的角度来看：自动化风险管理虽然会给企业带来一定的IT支出，但是它也在一定程度上减少了内部管控人员的配备，降低了公司的运营成本，因此其综合成本还是相对较低的。此外，自动化风险管理模式的平台化应用，有利于企业风险管理自评的推广，能够让更多人员参与到风险管理体系中，从而建立起风险管理的多道防线。

以成本控制为例，我们可以通过以下两个情景进行模拟分析：

情景1：ERP系统中的用户权限申请过程：
假设：一个有2000个SAP用户的企业，平均每月有100个用户变更需求（新增/删除/权限变动/锁定等），平均每个变更需求需要3位管理层审批和1位IT人员配置。管理层每月工资20000元，IT人员每月工资5000元，每月工作时间20天，每天工作8小时。该场景下企业围绕SAP GRC方案 部署了全面且自动化的企业风险管理和内部控制体系。表一列示了部署前和部署后的成本比较情况：**情景2：某业务流程中部署了自动控制代替手工控制措施：**

表1.GRC方案部署前后人工成本比较情况

	部署前	部署后
管理层平均审批时间(A)	20分钟（涵盖岗位核对，不相容权限校验，因外出而等待等情况）	3分钟（系统的不相容权限校验自动完成，能上网就可以在线审批）
IT人员平均配置一次所需时间(B)	10分钟	2分钟（系统自动生效）
管理层平均小时工资(C)	20000/(20*8)=125元	20000/(20*8)=125元
IT人员平均小时工资(D)	5000/(20*8)=30元	5000/(20*8)=30元
每月人工成本((A/60*3*C+B/60*1*D)*100)	13000元	2000元

可见，部署后人工成本降低了11000元。

假设：某手动控制的测试频率为25个，每年企业内部审计/自我评估为2次，每年企业外部审计为2次。内部审计手工控制每个样本耗时3分钟，外部审计每个样本耗时5分钟。内部审计人员每月工资8000元，外部审计人员小时收费500元。 表二列示了部署自动控制代替手工控制前后每年在内部审计和外部审计上所花费的人工成本比较情况。

表2.用自动控制替代手工控制前后人工成本比较情

	部署前	部署后
控制活动的测试样本量(A)	25	1
企业内部审计/自我评估次数(B)	2	2
企业外部审计次数(C)	2	2
内部审计人员测试每个样本耗时(D)	3分钟	3分钟
外部审计人员测试每个样本耗时(E)	5分钟	5分钟
内部审计人员每小时工资(F)	8000/(20*8)=50元	8000/(20*8)=50元
外部审计人员每小时收费(G)	500元	500元
每年成本(F/60*D*A*B+G/60*E*A*C)	2200元	90元

可见，部署后每年成本降低2100元左右，降幅达95%。如果有50个手工控制活动被自动控制活动所代替，则每年节约成本可达10.5万元(2100*50=105,000)。

图2. 自动化风险管理实施路线图



制定适合企业自身特点的自动化风险管理目标

企业的情况千差万别，实现自动化风险管理目标不能一蹴而就，应该通过一整套专业的，且有效的路线图和方法论，来实现风险管理和内部控制体系的自动化或优化，从而确保该体系以更有效的方式，更低的成本，更透明化的程度去运作。

图2显示的四步骤的自动化风险管理实施路线图，可以有效帮助企业了解自身的基础水平，制定适合企业且行之有效的自动化管控优化方案，逐步实现风险管理的自动化，并最终帮助企业成为一家风险智能企业。

在评估企业当前的自动化风险管理成熟度的时候，图3所示的模型可供参考：

在初步明确了企业的自动化风险管理水平后，企业可以进一步通过德勤专有的自动化风险管理框架体系（参见图4），确定自动化风控工作的优化空间，制定并实施具体的优化策略。表3详述了自动化风险管理框架体系中各阶段的特点和优化空间。

图3. 企业自动化风险管理成熟度评估模型

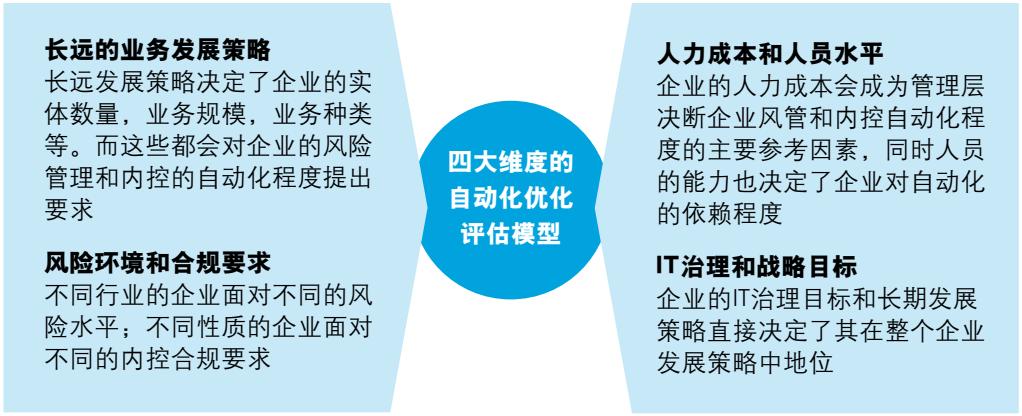


图4．自动化风险管理框架体系

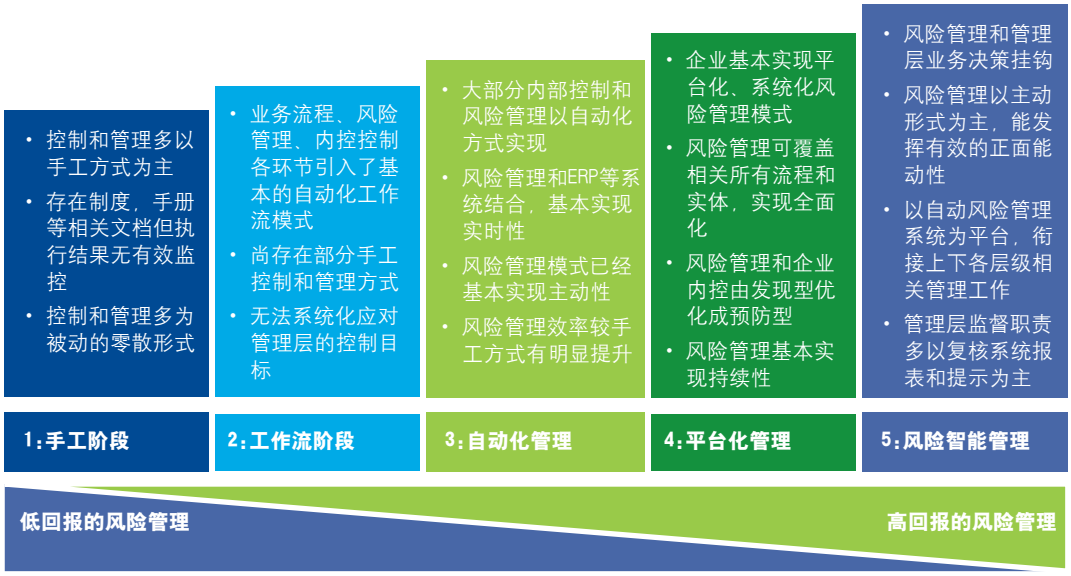


表3.自动化风险管理各阶段特点和优化空间

阶段	特点	风险管理和内部控制自动化的优化空间
1.手工阶段	• 控制和管理多以手工方式为主 • 存在制度，手册等相关文档但执行结果无有效监控 • 控制和管理多为被动的零散形式	• 根据自身需求和业务战略，形成初步的风险管控和内控发展目标和方向； • 实现关键业务流程初步自动化，例如实施ERP等系统实现销售订单/发票的自动化管理；采购订单/发票的自动化管理；存货出入库自动化管理。 • 实施系统过程中，关注业务流程中关键风险点和内控点的防范和合规遵循； • 通过应用系统、工作流、通讯技术把传统手工管理、工作流程自动化、提高流程效率并降低成本，例如采购订单审批工作流、权限审批工作流； • 基于系统原始数据，实施开发业务报表加强业务决策和管理有效性和及时性； • 建立风险管理和内部控制部门，提高团队专业能力，接受培训，通过自身力量或借助外部咨询团队实现跨越式发展。
2.工作流阶段	• 业务流程、风险管理、内控控制各环节引入了基本的自动化工作流模式 • 尚存在部分手工控制和管理方式 • 无法系统化应对管理层的控制目标	• 根据业务战略和已有情况，建立风险管控和内控自动化的清晰发展规划； • 深度、广度的继续业务流程的自动化、实现多系统、跨实体、跨职能的业务系统，整合、共享资源； • 系统实施过程中，基于风险评估、比较全面、系统的关注业务流程中关键风险点和内控点，并考虑自动化方式进行合规遵循； • 企业内管理类、工作流类流程基本实现自动化，考核、评价管理流程的执行效果和效率； • 基于大量业务和管理类原始数据，利用商业智能报表工具和平台执行初步数据分析、数据挖掘，为管理决策和自动化提供工作平台； • 风险管理、内部控制、内审部门强调系统流程的复核和审计，能动的在业务流程变更和系统流程变革中执行控制和合规职能。

阶段	特点	风险管理和内部控制自动化的优化空间
3.自动化管理	• 大部分内部控制和风险管理以自动化方式实现 • 风险管理和ERP等系统结合，基本实现实时性 • 风险管理模式已经基本实现主动性 • 风险管理效率较手工方式有明显提升	• 根据业务战略和内控风险管理水平，着手系统化、自动化风险管控和内控管理，培养主动的风险管理文化； • 按国内外先进标准和体系全面梳理企业业务、运营、管理流程中的主要风险管理和内控点，制定关键风险指标（KRI）和响应规则； • 开发、实施自动化工具与已有业务系统、管理类系统的对接和集成，采集、监督风险和内控相关的指标和数据，响应不利事件并预警，例如职责分离监测工具； • 借助系统平台部署风险管理和内控工作，把风险管理、内控、内审人员的主要工作系统化、标准化、透明化，包括风险识别，风险评估，风险应对和应对监管、内控自我评估、内控整改； • 基于业务数据、管理数据、风险内控监测数据、基于商业智能平台和工具开发各种报表和流程，便于管理层在业务决策就可以识别、评估、应对风险。
4.平台化管理	• 企业基本实现平台化、系统化风险管理模式 • 风险管理可覆盖相关所有流程和实体，实现全面化 • 风险管理和企业内控由发现型优化成预防型 • 风险管理基本实现持续性	• 根据业务战略和内控风险自动化水平，深入实施主动、量化的风险管理； • 建立整合的、全面的、符合国家要求和国际最佳实践的风险管理和内控系统平台，风险管理体系的各个方面都可以通过系统自动化实现，实现跨部门、跨实体的综合性应用； • 风险系统与ERP、管理系统、门户等系统全面集成，数据实时共享和传输，执行业务操作时就可以主动提示风险并分析； • 通过系统量化纯粹损失类风险，利用相关模型、关联矩阵等研究风险间相互关系和作用并通过系统自动化分析和处理，开展对有回报风险的合理利用； • 对业务部门风险管理进行绩效考核，并合理分配资源。
5.风险智能管理	• 风险管理和管理层业务决策挂钩 • 风险管理以主动形式为主，能发挥有效的正面能动性 • 以自动风险管理系统为平台，衔接上下各层级相关管理工作 • 管理层监督职责多以复核系统报表和提示为主	• 实现以股东价值最大化的风险管理和内控持续战略和文化，不断优化、调整企业的风险管理文化； • 建立全面风险管理体系和系统平台，把风险管理与企业战略、公司治理、IT治理等众多管理领域有机结合，实现风险信息系统和ERP、管理系统的全面整合； • 风险管理帮助企业能动、有效的执行业务决策，例如在新市场、新业务时通过风险历史事件数据库、实时业务数据的评估和分析、过程中的风险预警和监控等及时、全面的提供支持。

毫无疑问，风险智能管理，这一自动化风险管理的最终愿景，需要企业长期的探索和实践。但我们相信，只要企业迈出走向这一愿景的第一步，包括评估自身的自动化风险管理水平，制定初步的优化计划并付诸实施，企业将很快体验到自动化给企业风控工作所带来的“披坚执锐，快马加鞭”的效果；而当企业达到风险智能管理的境界，则可以从容地在波诡云涌的市场竞争中应对各类风险，最终，持续地提升股东价值！

本文已登载于德勤企业风险管理半月报第六期

ITIL信息服务管理最佳实务

温绍群　经理
德勤台北事务所
企业风险管理服务

在过去，信息部门在公司内部总是担任IT支持的角色，而到了网络时代，企业认识到信息技术可作为公司业务推广之一大助力，因此信息部门组织也随着使用单位的业务扩张而有所调整；除了原有的技术支持、系统维护等，加入了更多的业务功能分类，如负责电子商务或CRM系统等单位。但当信息部门所维护与管理的信息系统越来越多时，信息部门所必须处理的问题也随之增加，如何让问题的处理能够更有效果与效率，内部用户在寻求信息的协助时，不会因为负责的对口人员太多而无所适从，让信息部门人员从技术支持的角色转换为服务的角色，甚至将信息部门之服务有绩效可衡量，这些都是目前信息人员所面临的课题。本文将说明ITIL之概念、效益与导入方法，并提出一实例作为各位做参考。

ITIL简介

ITIL (IT Infrastructure Library)是一个发展了20年的信息管理实务，且迅速被IT界采纳为标准的方法，用来管理日益复杂的IT环境。这个广受欢迎的管理架构称为IT基础建设数据库。最初为英国政府在1980 年后期所发展的一套信息管理作法，包含了一系列的刊物，阐述以流程管理为主的最佳实务，并强调IT服务和信息系统之维运管理，藉由流程的改善与管理工具的搭配，达成企业绩效提升，由于 ITIL为一个模块化之信息管理实务，因此无论企业的规模以及所采用的技术，均适用于所有信息组织。因此，英国政府商务部(OGC: Office of Government Commerce)于2000年，协同英国标准协会(BSI: British Standards Institution)与IT服务论坛(itSMF: IT Service Management Forum)共同修订ITIL，促使BS15000信息管理标准与ITIL系列能互相的支持。

ITIL将信息流程模块化

由于ITIL为管理IT Infrastructure之最佳实务，其根本精神乃是将内部使用者当成顾客一样，强调信息之服务质量，而非单纯以技术支持的身份存在于企业中；因此，如同企业其他之重要营运流程一样，为了达到质量的提升，则需订定标准化之作业程序与关键绩效指针(KPI)，以为服务之持续精进。ITIL为了管理IT Infrastructure包含硬件、软件、组织沟通、程序、文件，与人员这些要件，将ITIL以10个管理流程模块与服务窗口(Help Desk)功能组织，来做信息基础之管理。

其中，Help Desk为信息单位面对内部用户之沟通平台。长久以来，信息部门常遇到的状况是，信息部门之专业人员将时间花在重复发生的问题上，而造成未能有效使用信息人员之人力，因此，使用Help Desk这样的作业模式类似于银行的客服中心，处理客户之抱怨与询问，将80%一般的call-in以过去历史数据所累积之知识库来解决，若有较难处理之事件，则交由较有经验之二线人员作问题处理，这样可将处理每个异常事件之单位处理成本降到合理水平，而达到内部顾客关系管理(Internal Customer Relationship Management)，其基本运作模式(如图1)。而Help Desk响应使用者之需求，包含：

- 与厂商或系统人员沟通，来解决使用者之问题。
- 监控信息基础系统。
- 提供用户相关之系统信息。
- 响应日常之用户电话求援或抱怨、事件处理与变更需求。

图1.服务窗口之运作模式

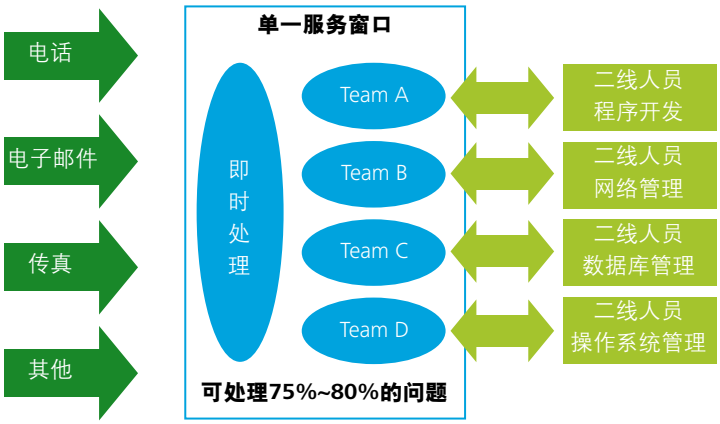
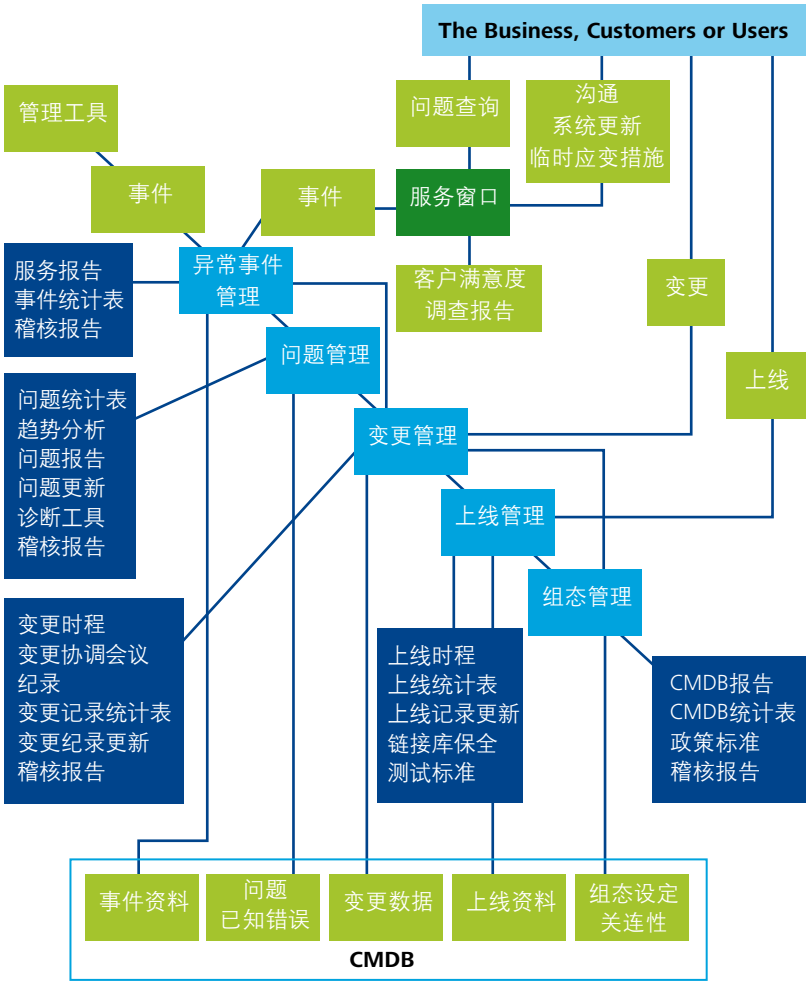


图2.信息服务支持流程



而ITIL的10个管理流程依其服务性质又可分为信息服务支持(IT Service Support)与信息服务交付(IT Service Delivery)。

一、信息服务支持 (IT Service Support) 包含:

- 配置管理 (Configuration Management)
- 事件管理 (Incident Management)
- 问题管理 (Problem Management)
- 变更管理 (Change Management)
- 上线管理 (Release Management)

ITIL的信息服务支持是以配置管理数据库(Configuration Management Database；CMDB)为基础，这个数据库会纪录管控之组件，如主机、网络、储存设备，甚至人员资料等，称之为配置组件(Configuration Items；CI)设定，透过配置管理流程，来建立并维护配置管理数据库，以确保其数据正确性，否则将因数据之不正确而导致分析错误，造成资源规划或使用浪费。随着CMDB的设置，信息服务支持之作业数据皆会储存于CMDB内，这些数据，将有助于Help Desk、各流程管理模块之相关人员进行问题处理、上线管理或变更作业。

举一个例子来说，某家全球化公司导入ITIL，其采用的Help Desk为Centralized 的设计，即全球分公司不管有何信息支持性问题，用户皆会将异常事件通知该Help Desk进行处理，程序如下所述(如图2)。

Help Desk会先将异常事件(Incident)登录至CMDB数据库内，由服务人员进行解决，并依照数据库内建之话术(script) 来回答使用者之询问，或是提供walk-around 的方式，让工作能尽快的持续进行，此为事件管理；然而，若是该类型异常事件不断的发生，则经过分析人员于数据库中进行趋势分析判断后，则可能将该事件"升级"至问题，而由相关之系统分析人员、网络人员或程序设计师进行问题之研究处理，甚至以一个项目来解决，追踪并找出事件的根本成因(Root Cause)，有些是属于已知 (Known) 的问题，有些属于未知(Unknown) 的问题，CMDB内都会加以管控，以供负责人员查询，此为问题管理；那些需要进一步更改到IT基础架构的变动，则需要提出变更需求(Request For Change；RFC)，经过核准后变更，此为变更管理；当需变更时，则会进行充分的计划与变更测试，以确保变更的有效性与效果的一致性，此为上线管理；以上的作业数据，都会储存于

CMDB中，做为分析与追踪查询的基础。ITIL的最高指导原则，乃是提高顾客的满意度，不管内部的支持流程是如何运作，都是要能够以提高客户价值为最优先，因此，需要定期的进行内部使用者满意度调查，来调整服务的内容与做法，以维持良好的关系。

二、信息服务交付（IT Service Delivery）：

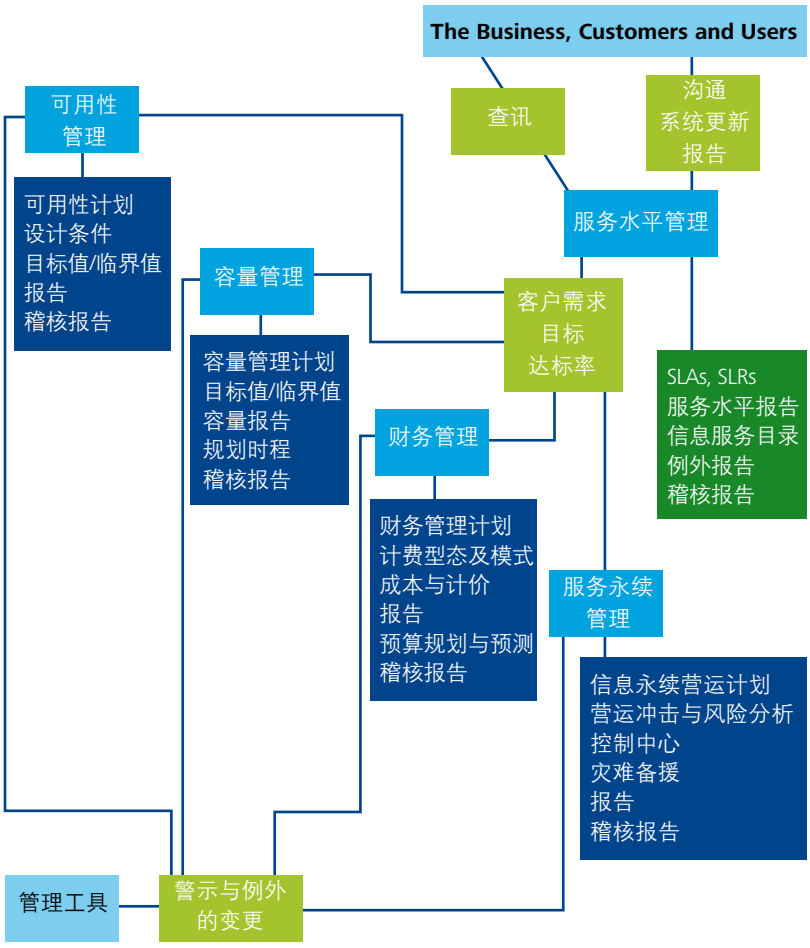
- 服务水平管理（Service Level Management）：
- 可用性管理（Availability Management）：
- 容量管理（Capacity Management）：
- IT服务连续性管理（IT Service Continuity Management）：
- 财务管理（Financial Management）：

综上所述，ITIL最高的指导原则乃是要满足使用者的需求，并提高其价值，然而，“满足需求”与“提高价值”该如何去量化并实行呢？这就必须要借由服务水准协定(Service Level Agreemen；SLA)来作为彼此双方价值沟通的基础。服务水平管理是面对客户(即使用者)时的核心观念，透过这个管理机制，可以决定出因应客户业务需求而所需提供的信息服务内容(即Service Catalog服务清单)，并且可以追踪这些需要的服务等级，是否有达到原先与客户拟定的服务水平，如果没有达到，再找出原因，确保达到与客户协议的目标，进而提升IT服务水平。也因此，可用性管理、容量管理、财务管理与服务连续性管理，都会依照客户的业务需求来拟订完善的作业计划与设定目标，这些活动都是为了能够达成服务水平协议的合约内容(如图3)。

举例来说，某家银行新设立了网络银行，这个网络银行经过市场调查与客户使用分析发现，网络银行网页的响应速度将会影响到客户的使用意愿。因此，网络银行的负责人员即设立了网页的响应时间不可高于 1秒钟之业务目标，然而，对于这样的目标，信息单位该如何去满足并达成？借由容量管理作业，设定容量管理计划(Capacity Plan)，同时考虑业务需求、目前之系统效能与信息技术更新等条件，并设定业务目标之临界值，由专门人员定期审核容量报告，才能做到事前规划，及早发现。

往往信息部门（或公司之管理阶层）会遇到的问题是，买了一些信息设备也投入了人力，却无法掌握住用户的质量要求，这是因为业务单位说的是业务需求，而信息单位说的却是系统效能等名词，无法达到有效的沟通。然而透过SLA的签订，将服务水平，如前述之网页响应时间不可高于1秒钟的目标，纳入SLA之requirement中，并明订罚则、定期报告与稽核等作业，透过这样的沟通平台，将会消弭很多业务单位与信息单位各说各话的纷争，真正的将心力放在提升外部客户的服务质量上。

图3.信息服务支持流程



ITIL导入效益

ITIL为协助企业进行信息部门之功能转型，执行以客户为导向(Customer-Oriented)的流程改善，因此，我们可从定量与定性二方面来看其导入效益。

一、定量效益：

可将异常事件的发生做有效的降低与处理：借由Help Desk将事件做有效的分类与初步解决，善用信息人员的能力与知识库，并提升解决问题的效率，让80%以上的异常事件可以在第一线人员就处理完成。

让信息成本结构以及信息定价模式清晰可见：

财务管理作业可协助企业将信息成本正确的分摊到各项目、作业与用户部门上，找出成本动因，可进一步说明信息之投资报酬(ROI)为何。

找出IT savings，以及可改善的空间：

由于信息成本结构的透明化，则可协助信息部门分析成本与效益，以降低 IT的成本，并合理化信息支出，重新分配信息的预算，争取额外的信息经费。

采取主动控制(proactive control)，极大化信息科技的投资报酬：

ITIL借由KPI的推行与各流程作业目标临界值的设计，让各相关人员能主动的去分析数据库内所记录之系统效能、抱怨事件与容量的使用等，积极提升信息服务品质。

二、定性效益：

因 ITIL为一个发展20年的最佳实务及标竿，以此标准来衡量公司的信息环境，将会更加提升公司之竞争力。导入ITIL将使信息部门关注业务单位之需求，让信息未来的发展方向与公司的策略更紧密的结合。让信息部门的价值更显而易见。借由单一服务窗口之设计，提高信息服务质量与信息人员之服务热忱。透过流程管理与工具的搭配与分析，让信息作业能达到预期的效果，而非只是理论。

ITIL导入参考

ITIL的导入，需考虑流程、人员与技术三个层面，而非一味的以导入信息系统为依归，笔者看过许多企业买了价值不菲的ITIL兼容的产品，却不知道ITIL需有管理流程相配合，甚至不知道ITIL为何，这样能发挥的效益实在有限。因此建议在导入ITIL时可先考虑以下各点：

- 任何的管理变革，要从企业之核心价值着手，尤其需将其效益与企业价值作align ，如此更能获得高层的支持。
- 应以内部顾客的角度，重新思考信息部门在企业内部之定位，且ITIL的导入乃是构建一个服务为导向的信息流程，因此人员的认知与教育训练是关键，以强化变革触动。
- 诊断目前的信息环境、绩效与内部使用单位之满意度，是否有改善的空间。
- 以ITIL为参考实务，来评估现今状态 (AS-IS) 与理想 (TO-BE) 的差距，而非从零开始，在既有的基础上补强不足之处。
- ITIL的导入需有先后顺序，除了各流程模块之间有其关连性之外，更应考虑quick-win，实施原则为 " Think Big, Do Small, Deliver Quick"。须找出ITIL流程间的依存关系及链接，确认共享的数据。
- 由于ITIL各流程模块均会设计相关之负责人(Process Owner)与配合人员，而这些人员是兼职担任，因此须考虑Role & Responsibility的设计，并须讨论如何进行跨部门合作，或调整组织结构。
- 目前企业内部是否正在导入其他的管理制度(如BS7799)，应考虑其流程管理的依存性与同时导入的可能性。
- ITIL的导入攸关流程的改善与职权的设计，因此应考虑到导入项目团队于公司的角色是否独立。

ITIL导入实例

一、专案背景：

该公司为一家全球化投资银行，为两家银行合并之存续公司，希望Deloitte协助将合并后的信息流程标准化与优化，并进一步降低信息部门之成本。

二、项目导入方法：

由于该公司刚完成合并作业，因此信息部门存在不少工作与管控上的盲点，因此Deloitte在这个项目中，建议该公司应从信息部门在公司之价值厘清开始，

并导入ITIL最佳实务，采取“评估－设计－实施－运作”的阶段性方法。现将导入方法说明如下(图4，说明如下)：

评估：

这个阶段，须先厘清相关之利害关系人(Stakeholder)对于公司信息部门之价值，包含管理高层、内部使用者、外包厂商与信息部门人员，采用了使用者满意度之调查、同业比较(Benchmark) 与信息流程成熟度之评估(以ITIL为标准)等手法，进行差异分析 (Gap Analysis)，并将导入的流程模块Prioritize，据以拟定改善计划，规划先期导入 Help Desk(7X24X365 服务不间断)、事件管理、配置管理、服务水平管理与财务管理。这个阶段，除了导入流程的优先级之外，尤其重要的是将项目团队所提之改善计划与提升用户价值（如提升效率，减少成本）连结起来，并传达（或"销售"）给相关之利害关系人，寻求管理高层的支持，承诺资源之投入。

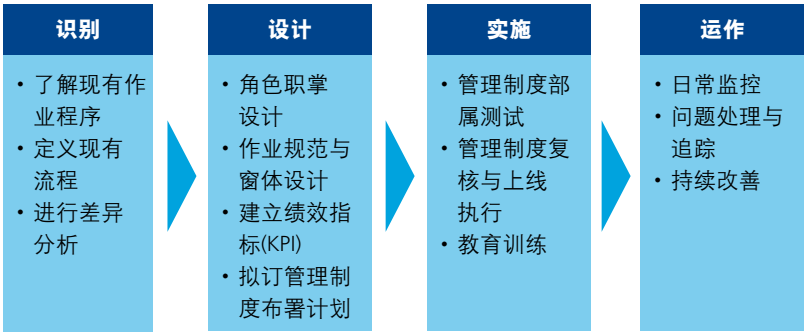
设计：

根据评估阶段所拟定之改善计划进行设计，除了流程之作业程序与管控的设计之外，设计了信息部门各作业流程之绩效衡量指针，为达成实时之监控与追踪，导入自动化管理工具。将流程的设计与工具互相整合，且由于相关之改变都会影响到现有信息人员与用户未来之作业流程与职权，因此，于实施前充分地沟通，降低人员抗拒改变的心理。

实施：

本阶段拟定实施计划(含D-Day计划)，包含流程、技术、管理等的布署，并于上线前，实施人员之教育训练与上线前的倡导，并选定pilot run的site，以测试模拟实施计划的完整性与设计的可行性，是否需要做调整，并实施风险与对策拟定。

图4. 敏感信息保护路图



运作：

随着使用者环境的改变，与服务水平要求的提升，对于原有的信息环境会造成影响，因此，须由各流程负责人员监控流程质量与服务目标达标率，持续改善流程、管理工具与信息人员之服务认知。

三、专案效益：

- 将原有信息部门因合并后存在的流程模糊点厘清。
- 将信息部门之作业成本做分摊，追踪并分析信息投资与预算执行情况。
- 由于订立出信息部门的作业绩效指针，而这个作业绩效指针是基于使用者的业务需求所拟定的，而提升了内部客户的满意度。
- 由于导入ITIL将信息部门的资源使用做实时与正确的容量分析，改善了信息预算的规划与信息成本的管理，而达到节省超过14亿美金成本的具体效益。

结论

信息部门在公司的角色，已从技术支持，进而转换成信息服务提供商，甚至是价值的创造者，信息人员、甚或是CIO该如何面对这样的一个挑战？ITIL提供了信息业界二十年的实务经验，这个实务经验已经过全球各产业大公司的验证，且不断地焠炼。最近，国内正如火如荼地进行金融改革，各大银行莫不通过彼此的合并整合，扩张势力版图与竞争力，然而无论是大并小或是小并大，面临到的将是信息环境的整合，管理流程的再造，因此，信息部门借由ITIL全球最佳实务的引导，提升IT服务效率与改善IT服务部门。

本文已登载于台湾财金信息双月刊

企业内部控制实务 (3)
—销售 (2) 收入确认、催款、收款

原国太郎　副总监
德勤上海事务所
企业风险管理服务

通过运用信息系统，提高业务与内部控制水平是所有企业的课题

应收账款：
谁都可能被虚增销售的诱惑拉下水

美国的安然事件、世通事件，日本的嘉娜宝事件以及中国的银广厦事件，都与虚假记录巨额销售收入有瓜葛，收入确认是现今内部控制要点的重点之一。确认收入是公司利润的来源，管理层凭一己之力轻易就能操纵产生大额销售收入额。而且，不只是管理层，子公司的总经理、部门主管、甚至是业务员，在迫于各种压力之下，都有可能在任何时候受利益驱使，进行虚增销售收入的操作。从外部审计人员的观点来看，“收入确认”也是审计的重点之一，需要投入更多的时间进行审计。

从内部控制方面来看，与收入确认相关的最关键的控制是针对收入确认的标准进行明确书面规定，并妥当制作，获取，保管作为收入确认依据的相关凭证。

“所有权及和所有权相关的风险合理地转移至买方的时点”是收入确认的基本原则。从这个意义上说，收入确认时点是按照销售合同上规定的条款为准；在中国，实务上也大多根据原则重视合同条款，有销售合同时依照合同，没有合同时以买方确认验收入库为准的情况较多。但是从实务角度说，国外许多公司实务上确认客户验收入库时点往往滞后，但更易把握自身的发货情况，而且由于国内送货途中的运输问题较少，因此从习惯上大多以发货时点为收入确认基准。但是当公司客户群固定，而且双方之间能够通过信息系统进行直接的数据交换时，将客户验收入库作为收入确认的基准是更加适当的。

在设备制造以及销售的行业中，有依照合同的出货时点为收入确认时点的、也有以按照安装完成后为收入确认时点的，另外还有先给予客户试用再确认销售等各种复杂的情况。这种时候就需要是从“所有权及和所有权相关的风险合理的转移至买方的时间点”的原则出发分析业务、根据收入确认的基准，妥当保管好相关凭证。

进行出口销售业务时，一般以单笔业务的国际商业贸易条款为依据确定作为收入确认的时点。母公司进行管理子公司之间的买卖时，根据不同的贸易条款，出口方应该等到从进口方传回单据后才能确认收入，但是由于后面章节讲到的提前结算的影响，必须要考虑可能漏记销售的情况。

此外，针对收入确认是否适当，应该尽可能成立独立的部门定期检查。具体讲就是对入账的收入进行抽样，确认作为收入确认基准的凭证以及数据是否存在、收入确认时点是否确切，同时检查下期初、月初有无非正常的退货。因为在期末记入销售收入，但在下一个期初再退货，以此虚增收入的作法，是一种常用而又经典的虚假记录收入的手法。

这些程序在外部审计当中是通常会使用的审计方法。由于收入确认的重要性，建议将该做法也作为公司的内部控制，并得以实施。[1]

开发票：
该业务流程在不同国家，区别巨大

开发票/Invoice以及收款，各国的商业习惯上有很大区别。

中国开发票的实务操作，与其他国家有着很大的不同，其流程有其独特之处。

无论是根据旧会计准则或者根据新的会计准则，销售并不是在开具发票之后才进行确认的，必须按照权责发生制的原则，确认销售（以及应收账款和销售成本）。这点是经常容易被混淆的概念。在确认销售同时，应该及时开具发票，但实务中如果未能及时开具发票，在进行纳税申报时，都必须填入“未开具发票”一栏中进行申报，税务局的纳税申报表上也有该栏。（进而言之，增值税也应该根据权责发生的原则，当确认销售时应该同时确认增值税销项税额）

在开具发票流程中，内部控制要求应该做到的是能够确保无遗漏地开具所有发票，为此可以针对开具发票申请以及财务记账凭证进行管理，并在开具发票之后对已开发票内容再做双重检查，确认有无盖上发票专用章。

然而，在与政府机关或者医院等进行往来交易时，一般先收到货物，支付货款完毕后，对方才开出发票。前面章节中也曾提到过，在中国国内，一般的企业间进行交易时，部分采用预付货款，在确认货款入账之后再进行发货并开具发票。发票只有在授信交易中，起到催付货款的作用。

在其他国家，开具Invoice(付款通知书)时，只是将请求付款内容打印在普通的纸张上，和一般的订单形式差不多，是为了催促对方付款，与销售确认和税金无关。而且如要进行修改或者取消（开具Credit Note），操作也很容易。

由于在很多行业中，付款通知书上的价格、付款条件、订单条款等项目与订单信息完全一致，实际上其就是根据“得到确认的（系统内部保存好

的）订单内容”自动打印而成。总之信息系统中用到最多的功能就是自动校验。反之，对于因频繁调价、订单内容和付款通知内容常常不一致的行业来说，在发出付款通知书以前，如果不经过盖章查看是不可能放心的，于是，这些行业往往在发出付款通知书之前会对其进行检查和批准。

总之，关于检查付款通知书的内部控制关键点是“付款通知书上的价格、付款条件是否正确，是否经过审批”。虽然中国的发票和国外的Invoice（付款通知书）本来起到作用各不一样，但是内部控制对于其基本要求是一样的。

除上述所讲的之外，各国在开具发票/Invoice以及确认应收账款流程中，主要有如下几点不同。

① 收款条件方面，欧美多是卖方在付款通知书中明确指定付款日期，一般使用的支付条款也只有仅有的几种到十几种。而与此相对，在日本，一般配合客户的情况有多种选择，客户月末结算的就在次月的某日支付的，或者15号结算就在次月末支付。在中国，采取先预收货款的交易模式比较多，当给与客户授信额度时，一般是要求对方在发票/付款请求之后一个月到三个月内进行付款。

② 发出付款通知书的时点方面，欧美基本是只开出一份随货的单笔业务的Invoice，中国也会按照一笔货物开出对应发票。与此相对，在日本大部分公司到月底也会另外发出正规的月度付款通知书。

③ 支付方式。在欧洲和日本基本以银行转账进行支付，然而在美国仍经常使用支票，委托外部有效率地进行收款。在中国，在进行大额国内支付时，基本上都使用银行转账进行支付，只有在小额采购时会使用转账支票。而据说意大利因建有全国共通的结算体系，支付方式又有所不同。

④ 对于延迟收款的确认。近年来，虽然日本企业和中国企业也开始导入欧美开发的集成化管理信息系统，对公司单笔业务出货确认应收账款，收款后单独进行核销；但是仍有企业是根据应收账款余额进行收款核销的。

对确认收款延迟的讨论

针对上述④确认收款延迟的问题，笔者之前曾与一位丹麦的会计师进行过探讨。这位丹麦会计师认为，对于将总的收款金额与应收账款余额进行核销时，会产生如下问题：

- 在应收账款账龄表（应收账款销账后余额表）中无法正确显示该笔逾期应收账款。
- 不能明确该笔货款究竟逾期多少时间，（对每月的应收账款余额整体进行核销时，只能了解每月应收账款的欠账额）。

上述案例中公司的信息系统是日本式的集成化信息系统，只能按每月总的收款金额来核销该月的应收账款余额，那么如果要满足这位丹麦会计师的要求，系统必须换成具有针对单笔业务进行核销功能的系统，或者对现有系统进行大规模的修改。[2]

这样、管理信息系统对于业务及内部控制都影响巨大。另外基于日本（或中国）的商业习惯而形成的业务模式以及内部控制，由于其与国际惯例不同，也往往不被认同。除上述例子之外，还有很多，不胜枚举。

并且，即使认同接受了这种以收款总额来核销应收账款余额的作法，并将其在业务流程以及内部控制中得以运行；但按照单笔出货来进行应收账款核销的方式，从管理角度来看更佳。

图3–1. 月度应收账款余额收款时的核销

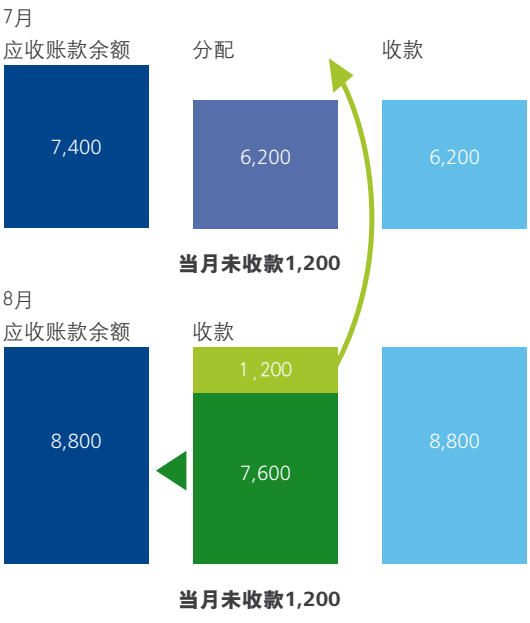
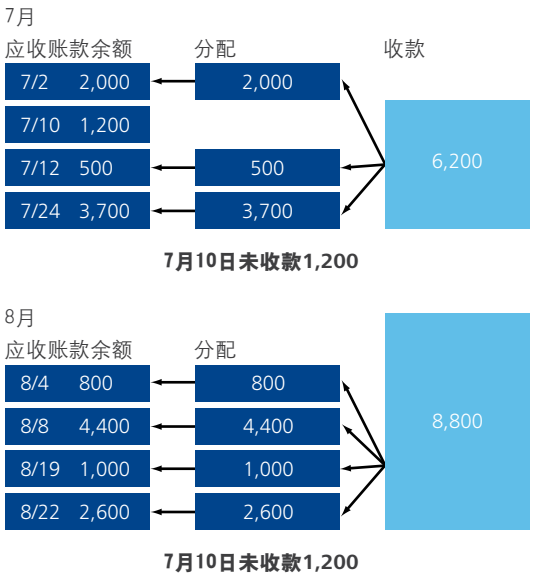


图3—2.以出库为单位计算的应收账款的收款核销



业务流程的处理速度及质量

过去，业务流程中，每月处理一次的工作较为常见。如每月一次制定销售、生产计划，落实库存、调配计划，月末财务编制科目余额表等。如今，人们越来越多的要求以更高的频度对计划等进行修正或处理，但是仍然还有很多企业对于各种业务维持每月一次的处理方式。

比如近年流行的供应链，通过该系统，将原本每月一次的业务，提速到每周一次、每天一次、甚至随时、其主要目的就是尽量减少业务流程从头到尾各环节的处理时间。如果没有网络和高度发达的管理信息系统，也不会有今天的高度商业化。

同样在会计行业，每季度决算的常规化和每月决算（并非科目余额试算表）的实施也是向同一个更实时的方向发展。其处理速度以及质量，受信息系统的运用是否到位和相关业务流程的设计是否合理，最终结果可能千差万别。

早前听到某个美国企业，在年度末之后3天内就完成了年末结账的工作。而且该公司的结账不仅是其单体，而是整个合并报表。

如前述的有关开具发票和确认销售的做法，通常的做法是每天的业务是开票，并且据此确认销售，然后只要每月一次核对本月实际发生的交易和开具发票的金额就足够了。但是这种做法仍有欠缺。如果财务会计系统能够自动与开票系统进行接口，将销售数据实时地导入开票系统，自动执行开票的话，业务效率更高，而且不要考虑月末执行人工核对，减少出错的可能性。

灵活运用信息系统以提高业务流程及内部控制的水准，应该是所有企业的必修课。

收款：能否信赖信息系统是个大问题

从业务销售实务的角度来讲，接到订单当然是最难的工作，在那之后的出货、发出发票、收款等程序可以说都是偏事务性工作的业务流程了。这样的工作如果能有效地运用信息系统，进行自动化、高效化整合是提高业务效率的关键。但是自动化系统尽管有利于内部控制的检验、检查等优点，也同时存在某些问题。

各行各业中，但凡一般的大型企业都会将收回货款与应收账款进行核对，然后考虑银行手续费造成的减额、折扣、到期日前的收款等种种因素，对应收账款进行核销。如果该工作完全依赖于手工作业，将是非常大的工作量。在中国国内，仍然有很多企业依靠手工作业来进行应收账款核销；国外的大型企业中，大多在信息系统中设定一定的条件自动进行应收账款核销工作，只有在实在核对不上的时候才由分管收款的人员会同销售业务员一起调查原因。

自动进行核销应收账款的首要前提是需要设定一个放宽的金额，例如预计的银行手续等，假设为30元。当收到货款与应收账款余额的容许误差在设定30元之内，则自动执行应收账款核销。

在欧美，很多公司为了提高工作效率，一般都将这个容许范围设定得较大。听说某英国公司，从新客户处收到第一个月的收款金额与应收余额有差额，但金额不大就没有向客户深究。但第二个月收回的货款与应收款的余额仍然存在差额，且比第一个月还要大，第三个月的差额索性更大。于是，公司和客户进行了沟通，结果第四个月的收款差额还是和第二个月的差额持平。虽然这也算不上是舞弊，但可以说是由于信息系统自动化产生的控制盲点的一个例子。

系统登录权限的限制是个重要的控制

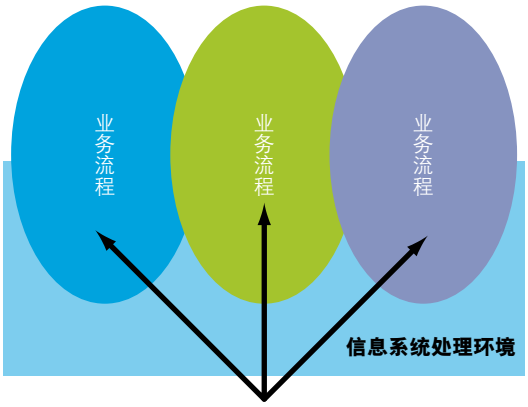
对于这样依赖于信息系统的业务流程来说，其内部控制流程只能建立在完全信赖信息系统的前提之上。

即使一个系统功能十分完善，如果任何人都有权限登录并能够修改其内容，其风险也是很大的。或者是一个系统的开发维护不到位，系统错误泛滥，在该系统中就无法保证相应功能的实现，包括诸如“依据经过批准的订单内容毫无更改地自动生成发票”、“根据发货数据正确记入收入、应收账款”。

销售循环中的舞弊行为，比如减少应收账款余额，将减少的金额与客户平分，或者截留收到的货款，等等，这类行为只要适当的设置系统登录权限，就能较大程度地遏制类似的舞弊行为。

诸如如何确保信息系统是否能够信赖，我们将其称之为“信息系统的整体控制”。

图4.不依赖信息系统的内部控制



依赖信息系统的内部控制

客户、供应商的主文档：对于主文档的控制是防止舞弊和失误的最后一道防线

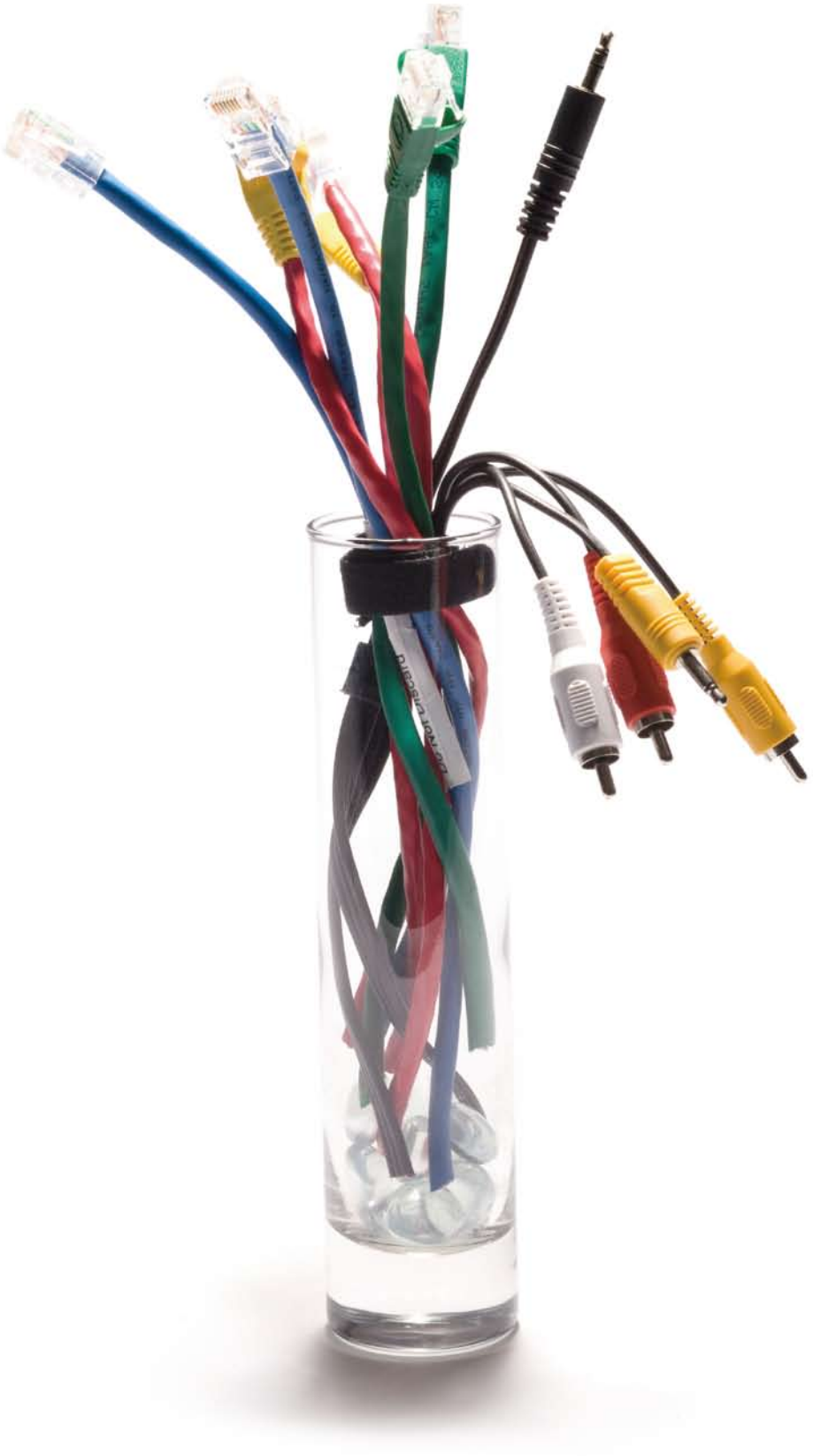
主文档是指在信息系统中事先登记录入的基本情况。比如客户主文档就有客户名称、客户收货地址、付款通知寄件地址、客户的业务人员名称、结算条款，还可能有信用额度、以及会影响销售价格的该客户分类等。另外在这里值得一提的是，供应商主文档中，可能包含和付款相关的具有很高风险度的信息，如付款银行账号等。

主文档的数据，由于在制作、处理单据时每次都会被引用、并被核对，因此保证主文档内容的正确性是非常重要的。另外，针对客户、供应商主文档，会由于管理不善，可能会造成不正当利用和产生成批错误，风险是很大的。相反来讲，切实有效地管理好主文档是防止舞弊及失误最后的一道防线。

关于供应商主文档，采购方虽将材料和商品的供应商单独登记在主文档中，但是发生零碎烦杂经费时，面对这些小的服务供应商时，就笼统地在系统主文档中虚设的一个公用户（杂项）。这种管理是非常不理想的。从内部统一管理的观点出发，事先未有效地登记供应商信息意味着每次付款时（各担当）都要一一输入供应商的相关信息，这必然伴随着相应风险的产生。同时，也可能在各项统计中发现“本公司本部门交易量最大的供应商竟然为杂项”。应尽量避免使用诸如上述的“杂项”供应商设置，而是能根据明文化规定来进行操作，严格管理。（夸张地说，为招待客户应酬而定点的饭店都最好能够设置相应的供应商主文档）

登录客户、供应商主文档以及变更主文档，都应经过适当的管理者的批准才能进行。批准登记主文档信息可以和新客户或新供应商的批准同时进行。此外，登录、变更主文档内容之后，最好由实际操作人员以外的人再对主文档进行核对。

在内部控制中更可能常常产生问题的，就是对客户、供应商主文档的未进行定期复核。为什么说这个会成为问题呢，因为实际上很少有企业能够做好这个工作。当客户和供应商数量众多时，从实务角度来看，定期对主文档的内容一一进行确认，确实比较困难；在加上如前述的对费用付款方要求也单独登记的话，定期对主文档的复核难上加难。



但是，要是抱着“登录变更之后再确认也可以”、“每天制作票据时都会引用相关内容，到时候再确认也不晚”这样的想法，是非常危险的。当负责登记、变更的操作员在录入批准后，又故意对已录入信息进行更改，或者存在长期未使用的主文档信息时，款项被汇入了已破产的供应商的银行账户，这种舞弊行为的后果不堪设想。

实际上当复核每一项主文档信息是很困难时，可以让系统自动统计打印出一定期间（前次复核开始至这次复核期间）的信息新增变更内容的报告，只对新增及变更部分进行复核，另外也可以通过程序实现以下功能：即对于一定时期没有使用过的客户或供应商，系统自动对其主文档信息进行冻结或者删除，像这样借助系统的力量代替人为内部控制也是可行的。但是每种方法都由各自的优缺点，应该结合实际，考虑选取最适合的功能及控制流程。

本文已发表于《中美日企业内部控制实务》一书中，但对其内容进行了些许调整。

1. 内部控制通常是为了确保能够产生正确的数据而形成的系统。但在这里针对的销售收入财务记录的复核，是对记录的数字金额进行抽样，和外部审计的程序完全一样，也许大家会稍许有点疑惑，为什么要求企业执行外部的审计程序。的确在内部控制程序中，即使是有些外部审计程序相当重要，单作为内部控制，一般并不被采用。但是正如正文所讲的，因为销售收入记录的重要性，建议公司内部的内部控制程序也一定程度上实施外部审计的程序。从学术上来讲，这种程序与外部审计相近，不是业务流程层面的内部控制。从内部控制要素的角度看，这不属于“控制活动”，而是“监督”这个要素。

2. 应收账款收款核销原本是公司必须作出判断的工作。当公司未能完全收款，不能进行核销时，与付款方进行确认才知道付款方的意图。也有可能是由于对方手头资金不足，而未能付足全部货款。因此调查逾期应收账款是一项非常重要的内部控制工作。

业务持续性管理 (Business Continuity Management)

陈建峰　副总监
德勤深圳事务所
企业风险管理服务

自踏入二十一世纪，911恐怖袭击事件及其后一系列灾难如SARS、美加大停电事件，乃至于无休止的网络病毒，都使企业管理高层将业务持续性管理列为议程首要事项。今日商业运营环境存在更多不可预见的风险，无论是为应对灾难抑或缩短正常营业流程的停滞期，均需要以全新方式重点优化所有关乎企业命运的重要资产－人才、流程、数据、技术和设施－关注是否在正常运营中强调对突发灾难或系统故障的应对。

业务连续性管理定义

目前国内外尚未有统一的针对业务连续性管理的定义标准和指引。以国际上流行的观点来说，如British Standards Institute (BSI) BS 25999-1:2006 Code of Practice for Business Continuity Management and BS 25999-2:2007 Specification for Business Continuity Management及BASEL High-level Principles for Business Continuity，业务连续性管理是以全局性管理流程的思想统筹应急响应、危机管理、灾难恢复及业务连续性等计划的管理方法。从业务连续性运营的角度出发，涵盖必要的应急响应计划、危机管理计划及包括灾难恢复计划在内的业务连续性计划。强调不管是应急响应、危机管理还是业务连续性管理，都不是单独的管理事件，而是不断完善的管理过程和机制，并注重高级管理层对应急响应、危机管理及业务连续性管理相关管理流程的责任归属。

企业要了解到业务持续性管理是一项全面及持续的过程管理，而不是一种简单的修修补补、一次性的、由一些独立的点所构成的方法论。作为现代企业全面风险管理的重要一环，业务连续性管理实际上是一种以"确保企业能持续运营"为脉络的管理思路，让企业能因应其业务独特性，加上企业治理、企业文化、变更管理、运营管理、信息系统管理等多方面所揉合而成的。坊间经常会有很多类似的技术用语，我们在下文中尝试以一案例进行阐述：

案例

当有应急事件或者突发事件发生的时候，一般组织的业务水平会骤然下降。这时由各个部门/分支机构所形成的第一层级将启动现场应急响应计划，并报告该部门/分支机构的应急负责人，再由应急负责人分析及评估是否有必要上报以进入危机管理程序。这个的好处是在没有造成更大的损失之前已经进行初步评估并处理。

当启动了危机管理程序后，有关突发事件会报告至危机管理负责人(即报告至组织危机处理最高领导层)，将会对该项突发事件对组织的损失和影响进行深入评估。并决定是否启动业务持续性计划，由各相关部门全力协助执行，包括其中的灾难恢复计划。高管将宣布该次事件为灾难并启动事先计划的报告程序。

从上所述的例子中，我们可以看到在业务连续性管理的领域中还有很多不同的术语，如：

应急响应计划 (Emergency Response Plan "ERP")

这是为应对突发事件、最小化突发事件对业务运作的影响和员工伤亡而采取的紧急行动和程序。

危机管理计划 (Crisis Management Plan "CMP")

这是在有危机事件的情况下，针对特定事故时各相关单位的角色和责任及协调决策和沟通的程序。其中也包括公共关系及危机沟通的活动。这些程序也会对有关损失评估及启动业务持续计划的条件。

业务持续计划 (Business Continuity Plan "BCP")

是为避免关键业务功能受到中断，减少业务风险而建立的一系列关键政策及程序，包括对支持关键功能的人力、物力和关键功能所需的最低保证资源，例如人员，关键记录，设备供给，工作场地，信息交流工具，技术以及其他共享服务等。

灾难恢复计划
(Disaster Recovery Plan "DRP")

是为了减少灾难带来的损失和保证信息系统所支持的关键业务功能在灾难发生后能及时恢复和继续运作所作的事前计划和安排。包括定义信息系统灾难恢复过程中所需的任务、行动、数据和资源的文件。用于指导相关人员在预定的灾难恢复目标内恢复信息系统支持的关键业务功能。

由于业务持续性管理所包含的内容和范围广泛，了解其中一些重要的术语，能使企业在推动有关业务持续性管理时有更透彻的认识和沟通。

业务持续性管理的重要性

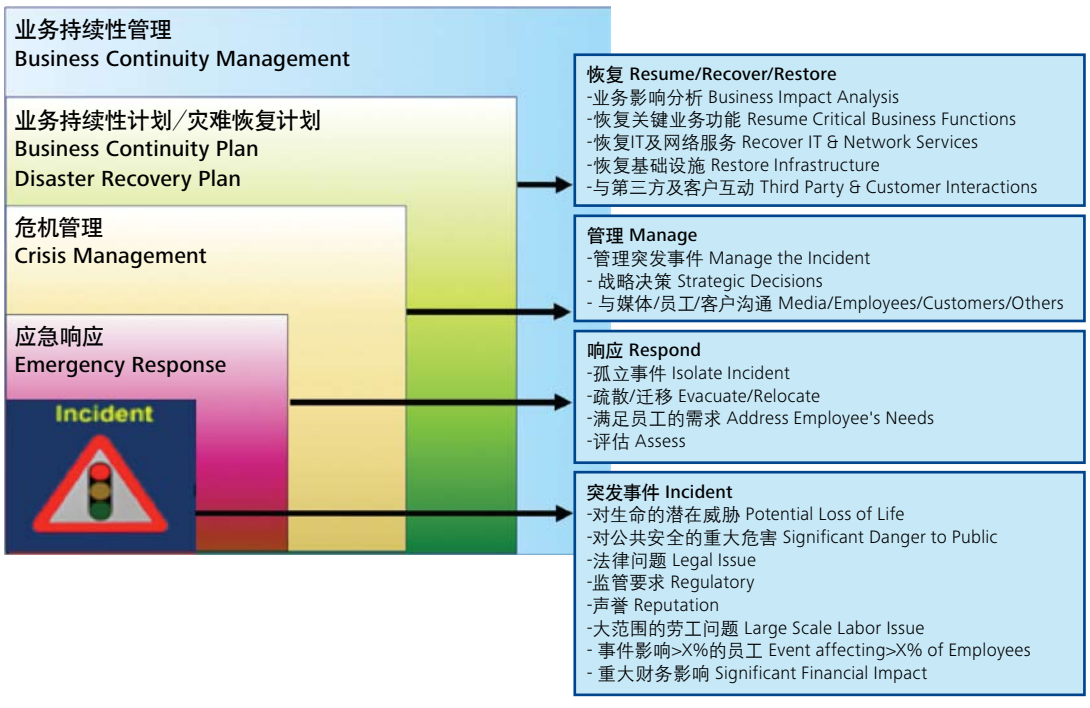
有效的业务持续性管理可确保意外事件(可对企业产生灾难性影响的事件)不致于干扰企业关键业务的运营。这意味着企业的客户服务、持续收入和股东价值在最不利事件发生时仍将受到妥善保障。

由于业务持续性规划旨在尽可能降低未知威胁的影响，如供应链崩溃、自然灾害、关键系统故障和关键人员失缺。常规的风险管理只能应对常规风险。业务持续性管理针对的是完全超出企业自身控制力的诸多风险。所以业务持续性规划和管理是企业面对所有不可缓解或不可规避、且通常不可投保的危险因素的最后一道防线。

附表

企业可以下列简单的几个问题以初步评估企业对业务持续性管理的准备水平：

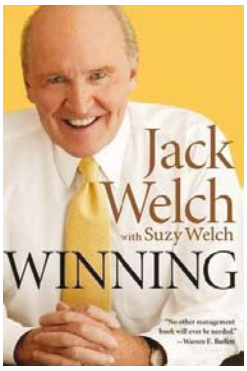
- 你的业务是否要求持续可用?
- 你是否已具有对所有方面进行恢复的计划?
- 你的计划是否充分考虑了人为威胁例如网络恐怖主义、破坏、等等的影响?
- 如果你不能再回到你的办公室，你怎么办?
- 你是否能重新部署你的办公场所和你的数据中心?
- 你的员工能否在家办公? 他们是否有所需要的信息和设备?
- 你能多快联系上你的员工? 你的关键客户? 你的供应商?
- 你是否已经评价过对一个或多个你的商业伙伴、供应商、服务供应商造成服务中断所带来的影响?
- 你与第三方服务供应商签订的合同/服务水平协议是否包含业务持续性要求?
- 你是否具备一个有效的程序防止和监测计算机中断/网络威胁?



赢 (Winning) 第四版

田晓静　经理

德勤香港事务所
企业风险管理服务



著者：
Jack Welch with
Suzy Welch

出版：
Harper

休假在家时翻阅了这本书，《赢 (Winning) 》。作为美国通用电气的前任CEO，杰克.韦尔奇在全球享有盛名。而《赢》这本书以充满韦尔奇特色的语言介绍了他的亲身管理实践经验，并结合了大量实际案例，如他在扉页里所说，“本书献给那些热爱商业生活、渴望把事业做好的人，献给那些每天一醒来就期盼在事业和生活中取得成功的人。”。

这本书涉及了企业管治及影响公司成长的各个重要方面，如公司战略、预算、领导力、人事管理、变革、危机管理等等。同时，它也为企业员工个人事业的提升和发展，以及平衡工作和生活提供了建议。而作为德勤企业风险管理服务部门的专业咨询顾问，我最感兴趣的是变革及危机管理这两个部分。

管理变革和危机管理是我们在工作中常常会提醒企业注意的重要问题，因为它不常在日常工作中发生，而容易被管理层忽略。在选择并推进变革的时候，本书介绍了4项实践方法：

- 在沟通中，说明每一项变革的合理原因；
- 有合适的人支持你的决定；
- 清除反对者；
- 抓住每一次机会，就算这是从别人的不幸中获得。

而在危机发生时，我们则需要在头脑中清醒地保持5个假设：

- 问题比表现出来的更严重；
- 世界上没有秘密，每个人最终都会知道所有的事情；
- 公众会用最负面的角度看待你和你的公司处理危机的方式；
- 工作流程和人员都将会产生变化，几乎每一次危机的结束都会付出沉重的代价；
- 企业会生存下来，并最终因此变得更为强大。

变革管理和危机管理都是企业风险管理方法应用的重要部分。其实，在企业的经营活动正常有序时，企业的管理者就应该问自己，你是否意识到变革和危机发生的可能性？你是否对相关的风险有清醒的认识和应对之良策？你和你的团队是否为此做好了准备？

如何在推进变革时，能够得到足够且有力的支持？我认为首先需要对公司所处的环境和变革面临的各类风险进行分析，分清利弊。并在风险分析的基础上制定相应的风险缓解计划，并对计划的施行进行监控。有严密的分析、计划和监控措施，才可以确保工作的合理可行，从而争取到企业里更多的人理解和支持变革活动，并积极参与其中。对既定程序和人员的重新整理，有效的变革往往是公司新一轮成功的开始。

如何在危机发生时，做到沉稳的应对？如书中所说，只要公司是由人组成的，错误就可能存在，意外、偷窃、欺诈就可能发生。危机的化解与企业的充分准备不无关系。公司应该在风险分析的基础上建立有效的内部控制系统，并建立危机应急管理体系，及公司持续经营计划。在意外发生时，才不会混乱不堪，而是可以快速的理清思路，按制度，有计划有步骤地处理问题。这样也有利于增加问题处理过程的透明度，在危机处理过程中让公司的诚信度和企业的凝聚力获得加强。有效的危机处理同样也可以提升公司形象，赢得市场和大众更多的承认和追捧。

在这一系列的公司治理活动中，作为企业风险咨询顾问，我们的任务则是利用自身庞大的资源网络和丰富的行业经验，为公司提供有价值的建议，帮助公司建立更好的企业管治和内部控制体系。成为企业在赢得一个又一个成功的过程中不可或缺的伙伴！

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有限公司
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有限公司
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有限公司
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

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大陆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大陆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。

《企业风险》第3期读者调查问卷

1）针对以下方面，请您评价《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	☐	☐	☐	☐	☐
图片	☐	☐	☐	☐	☐
版式	☐	☐	☐	☐	☐
编读互动	☐	☐	☐	☐	☐

2）本期《企业风险（第三期）》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)
访谈－台湾土地银行信息风险管理经验交流	☐	☐	☐	☐	☐
2010全球安全调研报告	☐	☐	☐	☐	☐
企业安保：介绍企业安保风险抵御系统（增强版）	☐	☐	☐	☐	☐
管控IT风险，提升IT价值	☐	☐	☐	☐	☐
加强电子银行交易风险管理，提升客户安全体验	☐	☐	☐	☐	☐
Web应用安全，您再也无法忽视的风险	☐	☐	☐	☐	☐
双管齐下 高枕无忧－数据防泄露在行业中的应用	☐	☐	☐	☐	☐
新环境下的企业信息系统日志分析	☐	☐	☐	☐	☐
自动化风险管理	☐	☐	☐	☐	☐
财金咨询－ITIL信息服务管理最佳实务	☐	☐	☐	☐	☐
连载－企业内部控制实务(3)- 销售流程(2)收入确认、催款、收款	☐	☐	☐	☐	☐
业务持续性管理（Business Continuity Management）	☐	☐	☐	☐	☐
推荐书籍－赢（Winning）第四版	☐	☐	☐	☐	☐

3）您最想了解的关于风险管理和企业内部控制的相关内容（可多选）

☐ 全面风险智能服务　☐ 资本市场服务　☐ 合规性准备及协助　☐ 业务持续性规划　☐ 信息治理

☐ ERP控制　☐ 安全电子商务　☐ 内部审计　☐ 合同风险与履约　☐ 计算机审计

☐ IT尽职调查　☐ 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内部刊物以及宣传资料？（☐ 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刊物发送名单中：

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《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)
	☐	☐	☐	☐	☐

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 《企业风险》出版委员会 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有限公司 企业风险管理服务《企业风险》出版委员会 收
谢谢您的阅读与合作！

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140个国家，凭借其世界一流的专业服务能力及对本地市场渊博的知识，协助客户在全球各地取得商业成功。德勤约170,000 名专业人士致力于追求卓越，树立典范。

关于德勤中国

在中国，我们通过德勤·关黄陈方会计师行和德勤华永会计师事务所有限公司，以及其下属机构和关联机构提供服务。德勤·关黄陈方会计师行及德勤华永会计师事务所有限公司共同为德勤有限公司的成员所。

德勤中国是中国大陆及港澳地区居领导地位的专业服务机构之一，共拥有逾8,000名员工分布于包括北京、重庆、大连、广州、杭州、香港、澳门、南京、上海、深圳、苏州、天津、武汉和厦门在内的14个城市。

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，我们更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、其任何成员所或上述其关联机构（统称为“德勤网络”）提供任何会计、商业、财务、投资、法律、税务或其它专业建议或服务。本文件不能代替此等专业建议或服务，读者亦不应依赖本文件中的信息作为可能影响自身财务或业务决策的基础。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。

©2011德勤华永会计师事务所有限公司
SH-006SC-11

这是环保纸印刷品