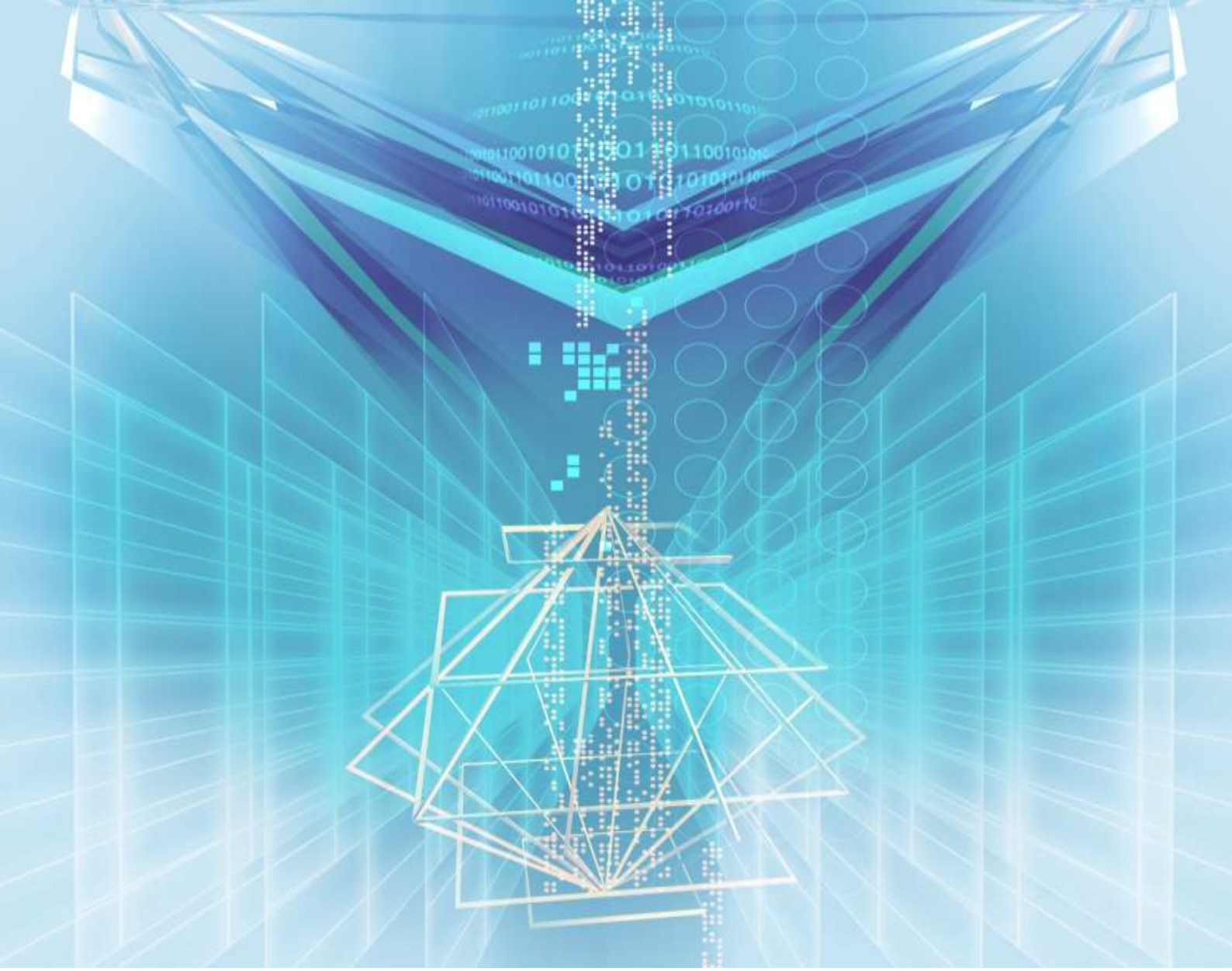


锐思咨询

Less Risk, More Value

锐思 · 视野

信息化风险专题

2013 年秋季刊（总第 9 期）

目　录

法规解读

方法指南

他山之石

案例解读

概念释义

法 规 解 读

国际 IT 治理常见标准

（锐思咨询 IT 服务部）

当今，企业的业务运营已经非常依赖于 IT 系统，IT 治理已经被很多企业所重视，通过 IT 控制帮助企业进行治理，在很大程度上节约了运营成本，控制了人为风险，加快了企业运营的效率。

近年，国际范围内已经出现了许多不同的 IT 治理标准，这其中很多治理标准已经成为企业用来进行管理的框架指引，也同时成为我国公司在治理过程中所值得借鉴的最佳实践。本文通过对国际常见 IT 治理标准进行整理，希望能对我国公司在实施 IT 治理方面提供思路和启示。（如表 1 所示）

表 1 国际常见 IT 治理标准

标准名称	发布机构	发布时间
内部控制整体框架	COSO	1992
COBIT	ISACA	1996
ITIL	CCTA	20 世纪 80 年代
ISO/IEC 38500	ISO/IEC	2008
ISO/IEC 20000	ISO/IEC	2005
ISO/IEC27000 系列	ISO/IEC	1995
PRINCE2	英国政府商务部	1989
TOGAF	The Open Group	1995

一、COSO 内部控制整体框架

1992 年，全美反舞弊性财务报告委员会发起组织（COSO）发布了内部控制整体框架，作为针对企业内部控制框架的指引性文件，在很多企业的内控建设中，起到了关键的指引作用，2013 年 COSO 发布了最新版的内部控制框架。

COSO 内部控制整体框架主要由五部分组成：

1.控制环境（Control environment）

它包括组织人员的诚实、伦理价值和能力；管理层哲学和经营模式；管理层

分配权限和责任、组织、发展员工的方式；董事会提供的关注和方向。控制环境影响员工的管理意识，是其他部分的基础。

2.风险评估（Risk assessment）

是确认和分析实现目标过程中的相关风险，是形成管理何种风险的依据。它随经济、行业、监管和经营条件而不断变化，需建立一套机制来辨认和处理相应的风险。

3.控制活动（Control activities）

是帮助执行管理指令的政策和程序。它贯穿整个组织、各种层次和功能，包括各种活动如批准、授权、证实、调整、经营绩效评价、资产保护和职责分离等。

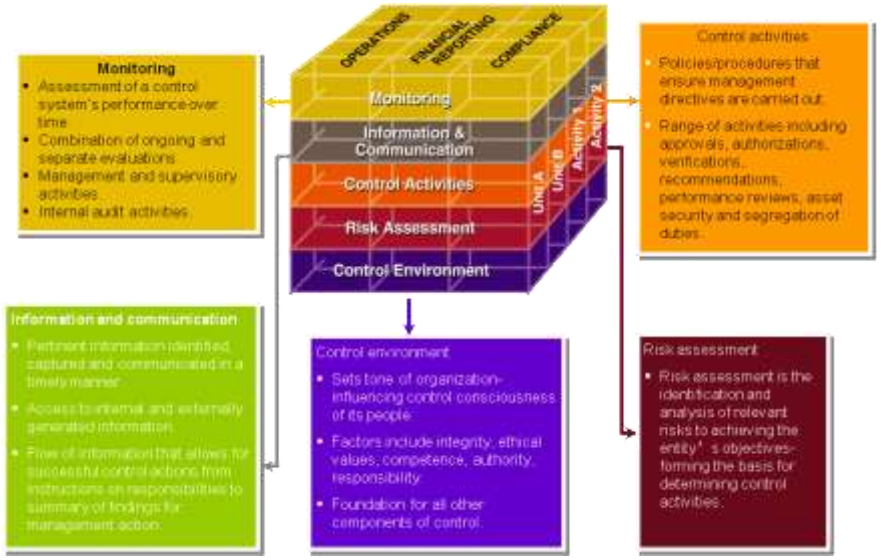
4.沟通与交流（Information and Communication）

信息系统产生各种报告，包括经营、财务、合规等方面，使得对经营的控制成为可能。处理的信息包括内部生成的数据，也包括可用于经营决策的外部事件、活动、状况的信息和外部报告。所有人员都要理解自己在控制系统中所处的位置，以及相互的关系；必须认真对待控制赋予自己的责任，同时也必须同外部团体如客户、供货商、监管机构和股东进行有效的沟通。

5.监控（Monitoring）

监控在经营过程中进行，通过对正常的管理和控制活动以及员工执行职责过程中的活动进行监控，来评价系统运作的质量。不同评价的范围和步骤取决于风险的评估和执行中的监控程序的有效性。对于内部控制的缺陷要及时向上级报告，严重的问题要报告到管理层高层和董事会。

在 COSO 的框架中，其基于的是传统针对财务报告的内部控制，主要关注的企业的业务流程，框架中主要在“控制活动”与“信息与沟通”对企业的 IT 治理进行了相关规定。



二、COBIT 信息系统审计标准

COBIT(Control Objectives for Information and related Technology) 是目前国际上通用的信息系统审计的标准，由信息系统审计与控制协会在 1996 年公布，并于 2012 年更新最新版 COBIT5.0。

COBIT5.0 是一套完整的、全球公认的、用于治理和管理企业信息和技术（IT）的框架，该框架支持企业行政层和管理层确定和实现其业务目标和相关的 IT 目标。COBIT 描述了五项原则和七项动力，用以支持企业开发、实施、和持续改进以及监控良好的 IT 相关的治理和管理实践。

COBIT 的目标主要在企业战略目标与 IT 目标之间建立起桥梁，使 IT 目标与企业的战略目标保持一致。COBIT5.0 中主要提到了如何根据利益相关者的需求，利用平衡记分卡从财务、客户、内部、学习和成长四个方面分别将企业目标与 IT 目标相互映射，体现了从企业的治理目标逐步分解到企业业务目标，企业业务目标再逐步分解成 IT 目标的过程。

同时，COBIT 覆盖了从分析和设计到开发和实施到运营、维护的整个过程，可具体应用到几乎所有企业信息系统中。

三、ITIL

ITIL 即 IT 基础架构库(Information Technology Infrastructure Library, ITIL，信息技术基础架构库)由英国政府部门 CCTA(Central Computing and Telecommunications Agency)在 20 世纪 80 年代末制订,现由英国商务部 OGC(Office of Government Commerce)负责管理，主要适用于 IT 服务管理（ITSM），2007 年 5 月 30 日，发布了了最新版 ITIL V3。ITIL 为企业的 IT 服务管理实践提供了一个客观、严谨、可量化的标准和规范。

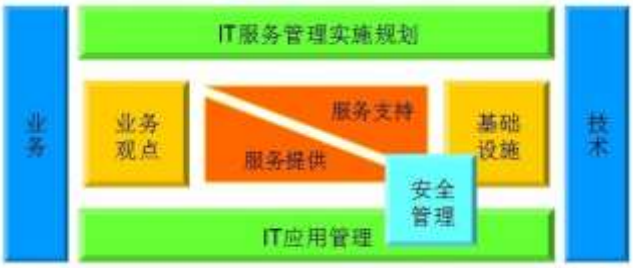
ITIL 是一套主要研究有关 IT 服务管理的方法。主要分为 Service Delivery 和 Service Support 两大部份。

Service Delivery 是属于战略性的思考，偏管理规范或协议，共分五大流程，分别是服务水平管理(Service Level Management)、财务管理(Financial Management)、可用性管理(Availability Management)、容量管理(Capacity Management)、持续性管理(Continuity Management)等

Service Support 是属于操作面规范，也分为五大流程，分别是事件管理(Incident Management)、问题管理(Problem Management)、配置管理(Configuration Management)、变更管理(Change Management)、发布管理(Release Management)

ITIL V3：主要结合 IT 服务管理生命周期 (Service Life Cycle)的观念扩增为５个核心模块，分别是服务策略(Service Strategy, SS)、服务设计(Service Design, SD)、服务转移(Service Transition, ST)、服务运营(Service Operation, SO)、持续服务改善(Continual Service Improvement, CSI)。

ITIL 为企业的 IT 服务管理实践提供了一个客观、严谨、可量化的标准和规范，企业的 IT 部门和最终用户可以根据自己的能力和需求定义自己所要求的不同服务水平，参考 ITIL 来规划和制定其 IT 基础架构及服务管理，从而确保 IT 服务管理能为企业的业务运作提供更好的支持。对企业来说，实施 ITIL 的最大意义在于把 IT 与业务紧密地结合起来了，从而让企业的 IT 投资回报最大化。



四、ISO38500

ISO/IEC 38500:2008 corporate governance of information technology -信息技术的组织治理- (以下称 IT 治理)，其主要衍生于澳大利亚 AS8015 标准。作为现有澳大利亚标准 AS8015 的快速跟随者，于 2007 年首次发布。2008 年 4 月该标准官方正式更名为 ISO/IEC 38500。

ISO/IEC 38500 是一个国际标准，用来指导 IT 管理。ISO/IEC 38500 标准提供了广泛指导方针和组织中进行 IT 监督的实施框架。ISO/IEC 38500 标准的目的是使 IT 治理成为公司治理的重要组成部分。

ISO/IEC 38500:2008 提供指导企业高层管理者（包括所有者、董事会成员、董事会董事、合作伙伴、高级管理人员，或其他人）在企业中使用有效、高效的，并可接受的 IT 原则。

ISO38500 核心内容是 IT 治理的 6 个原则及 IT 治理模型。

IT 治理的 6 个原则包括职责分工、IT 支持组织发展、可获得性、可用性、合规性、以人为本。

ISO/IEC38500 治理模型主要包含以下三点：

评估：领导层者应该检查和评判当前和将来的 IT 应用，包括策略、建议和供给安排（不管是内部、外部，还是两者都有）。在评估 IT 应用时，领导层应该考虑业务的内外部压力，如技术变更、经济和社会发展以及政治等方面的影响。领导层还应考虑当前和将来的业务需求、组织必须达到的目标以及战略或意图的特定目标等；

指导：领导层应履行指导制定计划和方针并指导实施的职责。计划应该设定 IT 建设项目和 IT 持续运营的投资方向。方针应明确期望的 IT 应用行为。领导层应确保“建设转运维”的过程置于有效的管控之下，且充分考虑对现有业务、IT 基础设施、应用系统及操作习惯的影响。领导层应以符合组织的指导及良好治理的六项原则，来要求管理人员提供及时的信息，鼓励组织内善治的 IT 治理文化。

监控：领导层应依据科学的监视体系评价 IT 的绩效，同时，鉴证 IT 合规过程。确保 IT 满足合规要求（法律、法规以及合同）和内部实际工作的需求。

五、ISO20000（BS15000）

ISO20000 是基于 ITIL 最佳实践与 BS15000 英标体系进行构建的，并于 2005 年 12 月由 ISO 组织发布的第一部具有国际权威性的 IT 服务管理体系标准。此套体系规范秉承“以客户为中心，以流程为导向”的服务理念，旨在帮助企业组织能够有效的识别与管理 IT 服务管理的关键过程

ISO/IEC20000 是一个关于 IT 服务管理体系的要求的国际标准，它帮助识别和管理 IT 服务的关键过程，保证提供有效的 IT 服务满足客户和业务的需求。

ISO20000 标准包括了 5 大过程，13 个管理面，150 多个核心控制点，如下所示：

1.服务交付过程：

> 服务等级管理

> 服务报告

> 能力管理

> 服务持续性与可用性管理

> 信息安全管理

> IT 服务预算编制与会计核算

2.控制过程：

> 配置管理

> 变更管理

3.发布过程：

> 发布管理

4.解决过程：

> 事故管理

> 问题管理

5.业务过程：

> 业务关系管理

> 供应商管理

六、ISO27000 系列标准

ISO/IEC27000 标准是国际标准化组织专门为信息安全管理体系建立的一系列相关标准的总称。

ISO27001 是 ISO27000 系列的主标准，ISO/IEC27001 的前身为英国的 BS7799 标准，该标准由英国标准协会于 1995 年 2 月提出，并于 1995 年 5 月修订而成的。1999 年 BSI 重新修改了该标准。

BS7799 分为两个部分：BS7799-1，信息安全管理实施规则 BS7799-2，信息安全管理体系规范。第一部分对信息安全管理给出建议，供负责在其组织启动、

实施或维护安全的人员使用；第二部分说明了建立、实施和文件化信息安全管理体系的要求，规定了根据独立组织的需要应实施安全控制的要求。目前，在信息安全管理体系方面。

国际标准化组织在 2005 年发布了 ISO/IEC 27001，ISO/IEC27001 信息安全管理体系标准已经成为世界上应用最广泛与典型的信息安全管理标准。其中主要包括了 11 个章节：

1）安全策略。指定信息安全方针，为信息安全提供管理指引和支持，并定期评审。

2）信息安全的组织。建立信息安全管理组织体系，在内部开展和控制信息安全的实施。

3）资产管理。核查所有信息资产，做好信息分类，确保信息资产受到适当程度的保护。

4）人力资源安全。确保所有员工，合同方和第三方了解信息安全威胁和相关事宜以及各自的责任，义务，以减少人为差错，盗窃，欺诈或误用设施的风险。

5）物理和环境安全。定义安全区域，防止对办公场所和信息的未授权访问，破坏和干扰；保护设备的安全，防止信息资产的丢失，损坏或被盗，以及对企业业务的干扰；同时，还要做好一般控制，防止信息和信息处理设施的损坏和被盗。

6）通信和操作管理。制定操作规程和职责，确保信息处理设施的正确和安全操作；建立系统规划和验收准则，将系统失效的风险降到最低；防范恶意代码和移动代码，保护软件和信息的完整性；做好信息备份和网络安全管理，确保信息在网络中的安全，确保其支持性基础设施得到保护；建立媒体处置和安全的规程，防止资产损坏和业务活动的中断；防止信息和软件在组织之间交换时丢失，修改或误用。

7）访问控制。制定访问控制策略，避免信息系统的非授权访问，并让用户了解其职责和义务，包括网络访问控制，操作系统访问控制，应用系统和信息访问控制，监视系统访问和使用，定期检测未授权的活动；当使用移动办公和远程控制时，也要确保信息安全。

8）系统采集、开发和维护。标示系统的安全要求，确保安全成为信息系统的内置部分，控制应用系统的安全，防止应用系统中用户数据的丢失，被修改或

误用；通过加密手段保护信息的保密性，真实性和完整性；控制对系统文件的访问，确保系统文档，源程序代码的安全；严格控制开发和支持过程，维护应用系统软件和信息安全。

9）信息安全事故管理。报告信息安全事件和弱点，及时采取纠正措施，确保使用持续有效的方法管理信息安全事故，并确保及时修复。

10）业务连续性管理。目的是为减少业务活动的中断，是关键业务过程免收主要故障或天灾的影响，并确保及时恢复。

11）符合性。信息系统的设计，操作，使用过程和管理要符合法律法规的要求，符合组织安全方针和标准，还要控制系统审计，使信息审核过程的效力最大化，干扰最小化。

七、PRINCE2

PRINCE2 起源于之前的 PRINCE 项目管理方法。PRINCE 最早是在 1989 年由英国政府计算机和电信中心（CCTA）开发的，作为英国政府 IT 项目管理的标准。但是，它很快就被应用于 IT 以外的项目环境中。PRINCE2 在 1996 年作为一种通用的项目管理方法正式出版。

随着 IT 治理在全世界的蓬勃兴起，Prince2 作为 IT 项目管理高效的方法成为 IT 治理的重要支持工具。PRINCE2 为项目管理提供了一种结构化的方法。这种方法为管理项目提供清晰界定工作框架。PRINCE2 介绍了如何协调项目中的人和活动、如何设计和监督项目以及在项目发生变更的情况下如何调整的流程。每一个流程都详细标出关键的输入、输出和具体目标及要执行的活动，这为计划偏差提供了自发的控制。这种方法把项目划分为多个管理阶段，保证让所有资源得到有效的控制。依靠严格的监控，项目在控制和组织的方式下得到执行。作为一种被广泛认可和理解的结构化方法，PRINCE2 为项目中所有参与方提供了一种通用语言。它完整阐述了参与项目的各种管理岗位和职责，并可以根据项目的复杂程度和组织能力来适当调整。

PRINCE2 定义了 45 个单独的子过程，并把它们组织到 8 个过程中。

1.项目准备(SU)：在这个过程中，任命项目团队，准备项目概述文件（概括地描述这个项目要试图达到什么要求以及这样做的商业目的）。另外要决定采用

的整体方法，做下一个阶段的计划。

2.项目计划(PL)：PRINCE2 主张产品基于计划，意味着计划时第一个任务就是确定和分析产品。只有确定了需要创建这些产品的必需活动，才可能估算每个活动需要的时间，然后编制安排活动的计划。任何工作总有相关的风险并且要分析风险。最后，这个过程会表明项目能达到什么样安排的计划，并且确保计划按照安排来完成。

3.项目启动(IP)：这个过程建立在项目准备活动和项目概要文件补充形成商业论证的基础上。项目质量保证方法与项目整体方法保持一致，以确保项目控制。制定出的项目文件作为一个项目整体计划。也要建立项目下一阶段计划，在项目管理委员会授权项目之前要整理项目启动文件。

4.项目指导(DP)：这些分过程指出项目管理委员会（由项目主管等角色组成）应该如何控制整个项目。上文提到，项目管理委员会可以授权阶段启动，也可以授权项目。项目指导也指出项目管理委员会应该如何授权阶段计划，包括由于延误或其它不可预见的情况导致的原计划被替代的阶段计划。另外，还包括项目管理委员会可以做出什么特别指导和确认项目收尾。

5.阶段控制(CS)：PRINCE2 建议项目应该分解为多个阶段，而这些子过程指出应该如何来控制每个阶段。最基本的是这包括哪些工作包要授权和验收。它也详细指出哪些过程应该检查，过程要点如何报告给项目管理委员会。捕捉和评估项目问题的方式建议与纠正行动方案一起汇报。这也给出了哪些项目问题应该按规定逐级汇报给项目管理委员会的方法。

6.产品交付管理(MP)：这个过程包含 3 个子过程，涉及一个工作包的验收、执行和交付。

7.阶段边界管理(SB)："阶段控制（CS）"过程提出了在一个阶段内应该完成的内容，"阶段边界管理（SB）"提出在一个阶段结尾时应该完成的内容。最明显的，应该是编制下一个阶段计划，尽可能更新总体项目计划、风险记录单和商业论证。这个过程也涉及到超出阶段界限允许范围时应该完成的内容。最后，这个过程指出阶段竣工应该如何报告。

8.项目收尾(CP)：这涵盖了在项目收尾的时候需要完成的事情。项目将要正式解散（所有资源空出来给其它活动），紧接着确定后续活动，就项目本身正式

进行评估。

PRINCE2 提供从项目开始到项目结束覆盖整个项目生命周期的基于过程的结构化的项目管理方法，共包括 8 个过程，每个过程描述了项目为何重要（Why）、项目的预期目标何在（What）、项目活动由谁负责（Who）以及这些活动何时被执行（When）。

八、TOGAF

TOGAF 由国际标准权威组织 The Open Group 制定。The Open Group 于 1993 年开始应客户要求制定系统架构的标准，在 1995 年发表 The Open Group Architecture Framework (TOGAF) 架构框架。

TOGAF 的基础是美国国防部的信息管理技术架构(Technical Architecture for Information Management: TAFIM)。它是基于一个迭代(Iterative)的过程模型，支持最佳实践和一套可重用的现有架构资产。它可让您设计、评估、并建立企业的正确架构。TOGAF 的关键是架构开发方法（Architecture Development Method: ADM）：一个可靠的，行之有效的方法，以发展能够满足商务需求的企业架构。

TOGAF 从四个角度描述企业架构：

1.业务体系架构：业务策略，管理，组织和关键业务流程。

2.应用体系架构：被部署的单独应用系统、它们之间的交互、以及它们与组织核心业务流程之间关系的蓝图。

3.数据体系架构：企业逻辑和物理数据资产、数据管理资源的结构。

4.技术体系架构：软硬件逻辑上的能力，这些能力要求对业务、数据和应用服务的部署提供支持。该架构包括 IT 基础设施、中间件、网络、通信、处理流程和标准。

COBIT 框架的解读与应用

（锐思咨询 IT 服务部）

2012 年 5 月，ISACA 发布了 COBIT 的最新框架指引——COBIT5.0，作为目前国际上较为通用的信息系统审计标准，COBIT 框架的应用给企业在管理与 IT 治理之间搭建起了桥梁，从而连结了企业战略目标与 IT 目标，来帮助企业实现最大价值。

本文通过对最新 COBIT5 框架的解读，期望能在企业的发展过程中提供一些启示或建议。

一、COBIT 的发展历史

信息技术是所有企业的关键资源，当前信息的重要性和普遍性正日益成为企业管理的重要部分，企业的 IT 治理也逐渐被企业管理层所重视。有效的 IT 治理不但可以提高企业的管理水平，同时也能增强企业的竞争力。

COBIT 是美国 ISACA（信息系统审计和控制联合会）制订的面向流程控制的信息系统审计和评价的标准，是一个基于 IT 治理概念的、面向 IT 建设过程的 IT 治理实现指南和审计标准。ISACA 自从发布 1996 年发布 COBIT1.0 开始，到目前为止已经陆续更新到了 COBIT5.0，在这过程中，COBIT 从一种 IT 审计工具逐渐演变成了覆盖企业 IT 治理与管理的框架指引。（如表 1 所示）

表 1　COBIT 的发展历史

版本	发布时间	主要作用
COBIT 1.0	1996 年	作为一种 IT 审计指引首次发布。
COBIT 2.0	1998 年	在 1.0 的基础上增加了控制目标，明确了企业 IT 控制目标。
COBIT 3.0	2000 年	在 2.0 基础上增加了管理指南，COBIT 逐渐演变成企业的管理工具。
COBIT 4.0/4.1	2005 年/2007 年	在 3.0 基础上更加关注企业的 IT 治理，从企业的更高层来对 IT 进行管控，在 2007 年发布 COBIT 4.1，但并无更新内容。

版本	发布时间	主要作用
COBIT 5.0	2012 年	在 4.1 的基础上，对整个框架进行了调整和优化，从而全面覆盖了企业 IT 治理与管理的主要方面。

二、COBIT 5.0 解读

COBIT 框架试图在企业目标与 IT 目标之间，搭建起一座桥梁，将 IT 治理融入企业治理中，以此来全面覆盖企业运营过程中各个方面。

在最新版本COBIT 5 框架中，是以五个基本原则为基础创建而成的，企业可以以此来进行IT的治理和管理：

原则 1：满足利益相关者需要

企业的存在就是通过在实现收益、优化风险和运用资源之间维持一种平衡，从而为其利益相关者创造价值。利益相关者就包括了内部如董事会、经理、员工等以及外部如供应商、客户、监管部门等。创造价值就需要企业在降低风险的情况下，以最优的资源分配来实现收益。（如图2所示）

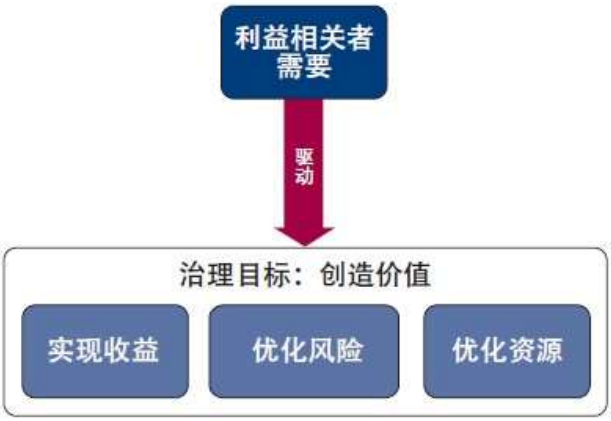


图 2 企业治理目标

在 COBIT 最新框架中，主要介绍了企业如何通过 COBIT 框架将治理目标逐步分解到企业目标，企业目标再逐步分解成 IT 目标，最后从 IT 目标分解成动力目标的过程。

这其中体现了 3 个过程：

治理目标——企业目标：COBIT 根据平衡记分卡，从财务、客户、内部、学习和成长四个方面分别定义了 17 项企业目标与治理目标之间的关系，详见下图

3。（图中 P 代表主要关系，S 代表次要关系）

BSC 维度	企业目标	与治理目标的关系		
		实现收益	优化风险	优化资源
财务	1. 商务投资的利益相关者价值	P		S
	2. 竞争性产品与服务的组合	P	P	S
	3. 管理的业务风险（资产保障）		P	S
	4. 外部法律法规的合规性		P	
	5. 财务透明度	P	S	S
客户	6. 以顾客为中心的服务文化	P		S
	7. 业务服务的持续性和可用性		P	
	8. 对变化的企业环境敏捷的反应	P		S
	9. 信息为本的战略性决策	P	P	P
	10. 服务交付成本优化	P		P
内部	11. 业务流程功能性优化	P		P
	12. 业务流程成本优化	P		P
	13. 管理的业务变更方案	P	P	S
	14. 运营及员工生产率	P		P
	15. 内部政策合规性		P	
学习和成长	16. 熟练的有进取心的人员	S	P	P
	17. 产品和业务创新的文化	P		

图 3 企业目标与治理目标映射表

企业目标——IT 目标：由于企业目标的实现需要若干个 IT 目标来体现，因此产生了企业目标与 IT 目标相互映射的关系，建立起企业目标与 IT 目标之间的桥梁，详见下图 4。

			企业目标																	
			商务投资的利益相关者价值	竞争性产品与服务的组合	管理的业务风险（资产保障）	外部法律法规的合规性	财务透明度	以顾客为中心的服务文化	业务服务的持续性和可用性	对变化的企业环境敏捷的反应	信息为本的战略性决策	服务交付成本优化	业务流程功能性优化	业务流程成本优化	管理的业务变更方案	运营及员工生产率	内部政策合规性	熟练的有进取心的人员	产品和业务创新的文化
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
IT 相关目标			财务					客户					内部					学习和成长	
财务	01	IT 与业务战略的一致性	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT 合规和对业务的外部法律法规合规的支持			S	P											P		
	03	行政管理层对进行 IT 相关决策的承诺	P	S	S					S	S		S		P			S	S
	04	管理的 IT 相关业务风险			P	S			P	S		P			S		S	S	
	05	从 IT 驱动的投资和服务组合中实现的收益	P	P				S		S		S	S	P		S			S
	06	IT 成本、收益和风险的透明度	S		S		P				S	P		P					
客户	07	符合业务要求的 IT 服务交付	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	应用程序、信息和技术解决方案的充分利用	S	S	S			S	S		S	S	P	S		P		S	S
内部	09	IT 敏捷性	S	P	S			S		P			P		S	S		S	P
	10	信息，处理基础设施和应用程序的安全			P	P			P								P		
	11	IT 资产、资源和能力的优化	P	S						S		P	S	P	S	S			S
	12	通过将应用程序和技术整合进业务流程之中来推动和支持业务流程	S	P	S			S		S		S	P	S	S	S			S
	13	准时，按预算提交收益和满足要求和质量标准的项目集交付	P	S	S			S				S		S	P				
	14	用于决策之可靠和有用的信息的可用性	S	S	S	S			P		P		S						
	15	IT 对内部政策的合规性			S	S											P		
学习和成长	16	胜任的有进取心的业务和 IT 人员	S	S	P			S		S						P		P	S
	17	业务创新的知识，专门技术和首创精神	S	P				S		P	S		S		S			S	P

图 4 企业目标与 IT 目标映射表

IT 目标——动力目标：实现 IT 目标需要若干个动力目标的支持，所谓动力即单个或几个可能对企业 IT 治理与管理产生影响的因素，也就是影响企业治理与管理的基本要素。在 COBIT 中描述了以下七种动力因素：

- 原则、政策和框架
- 流程
- 组织结构
- 文化、道德和行为
- 信息
- 服务、基础设施和应用程序
- 人员、技能和能力

原则 2：端到端覆盖企业

COBIT 5 框架将企业 IT 的治理整合进企业治理中，COBIT 5 可以全面覆盖企业内所有的职能和流程。COBIT5.0中，将企业的IT治理与管理划分为5个域37个业务流程。

这5个领域涵盖了管理层IT规划、建设、运行、监控以及企业治理层的指导

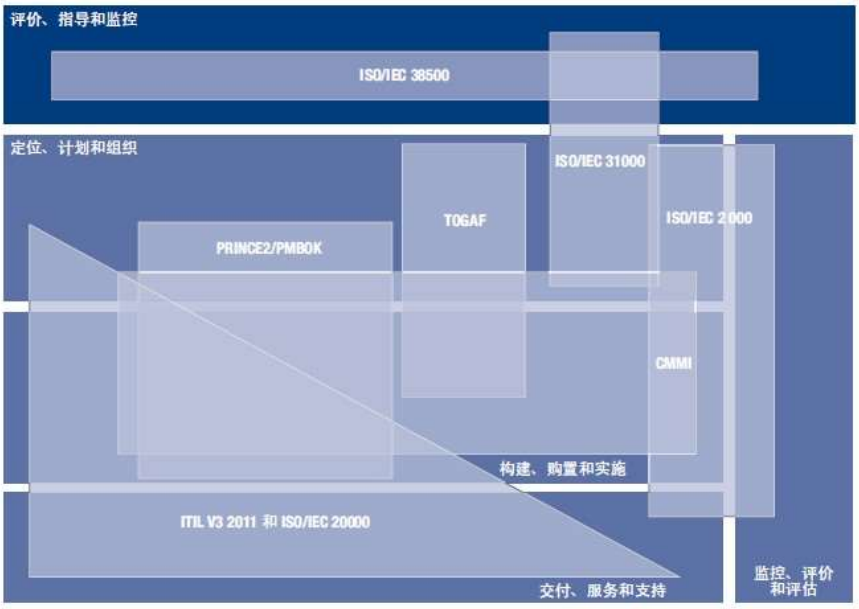
整个生命周期，每个过程都有清晰的控制目标、成熟度模型，明确了过程的角色和职责，将各种目标统一于COBIT控制模型。

原则 3: 运用单一整合式框架

COBIT5框架是结合ISACA过去所发布的框架指引以及国际上许多与IT相关的标准的最佳实践，才整合出来的。

首先，COBIT5将ISACA现有的框架指引进行了整合：其中包括COBIT4.1框架、IT价值管理、IT风险管理、信息安全商业模式等。

其次，COBIT 5 框架与其他国际IT相关标准保证了高度的一致，包括ISO/IEC38500、ITIL、PRINCE2等国际标准。（如图所示）



通过整合为单一的框架，使得COBIT5.0可以应用到企业的各个领域，包括IT审计、IT风险管理等等方面。

原则 4: 采用一个整体全面的方法

前文中提到，COBIT 5 定义了七个动力要素来支持企业IT的综合治理和管理体系的实施。所谓动力在广义上定义为任何能帮助实现企业目标的因素：

– 原则、政策和框架——作为比较基本的动力因素，其往往对企业战略发展起到了关键作用

– 流程——是企业需要达到战略目标所必经的过程

– 组织结构——是企业实际进行决策的基础

– 文化、道德和行为——会被企业所低估，而往往成为企业内部舞弊等事件的起因

– 信息——作为企业的资源，其贯穿于企业内外部的整体构架之中

– 服务、基础设施和应用程序——企业的硬件资源

– 人员、技能和能力——企业的软件资源

在这七个动力因素中，每个动力因素并不是孤立的，企业的运营可能会涉及到全部的动力因素。例如企业的信息安全，就会涉及到如流程、文化道德行为、基础设施、人员等等多个动力因素。

这些动力因素企业管理中是否起到了作用，在COBIT5中也明确每个动力因素绩效管理，本文以信息动力要素为例进行说明：

>信息涉及到的利益相关方是谁——即信息是否能满足利益相关方的需求，而信息所涉及到的利益相关方可能包括信息的生成者、信息的使用者、信息的管理者

>信息的目标是否能实现——即信息是否客观、真实、完整、安全或明确

>信息的生命周期是否予以了管理——即从信息的采集、分析、存储、使用和销毁

>信息动力因素是否得到了应用——信息是否经过分析后，通过某种载体予以了发布，从而为企业实现目标提供了参考，也即信息的价值是否得以体现。

原则 5: 区分治理和管理

COBIT 5 根据ISO/IEC38500标准将治理和管理明确区分开来。从 COBIT 5 的角度来看，治理和管理之间的关键区别在于：

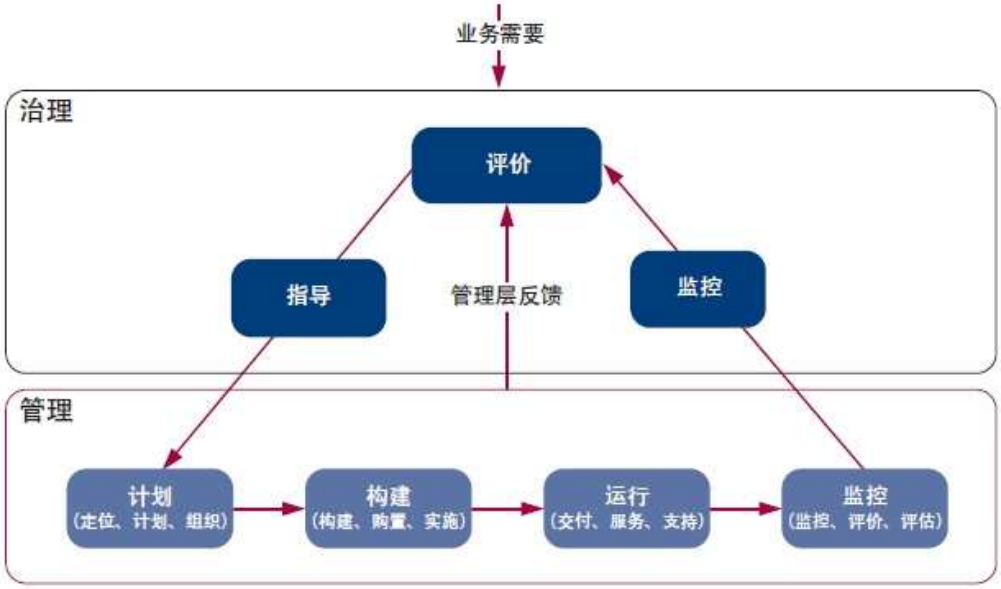
– 管理

管理层在既定的IT治理模式下，通过计划，构建、运行和监控来实现企业目标。大多数企业中，管理是首席执行官（CEO）领导下行政管理层的责任。

– 治理

治理是根据利益相关者的需要，而制定的整个企业IT规划组织、实施运行、服务交付以及监控评估的整体框架。在大多数企业中，整体治理是董事长领导下的董事会的责任。具体的治理责任可能授予适当级别的特别组织结构，尤其是在

较大型综合性企业中更是如此。



三、COBIT 在我国应用情况

目前，我国的企业信息化进程相对于其他外资企业来说比较滞后，企业的运营如今已经越来越依赖于信息化的建设，成熟化的信息化治理体系，不但能够促进企业进行有效的内部控制，更能在一定程度上提高企业经营效率效果。

COBIT 作为国际上十分成熟的 IT 治理框架指引，为企业的 IT 治理提供了强有力的理论基础，对于未来我国企业信息化进程，也起到了指导作用。

1.作为提高企业经营效率效果的工具

2008 年我国五部委颁布了《企业内部控制基本规范》，其中第 18 号指引《信息系统》中特别提到了企业应将信息化的建设提到企业管理中更加重要的位置。在最新的 COBIT5.0 框架中，建立起了战略目标与经营目标的映射以及经营目标和 IT 目标的映射，将企业的治理目标逐步分解成七个动力目标，再根据动力的绩效管理，明确了动力要素的目标、职责、过程管理等，从治理与管理的角度共同进行控制。

一旦这样从治理到管理由上而下的体系建立起来，企业的信息化建设就能根据战略目标落实到具体的环节，帮助企业提高管理水平。

2.作为企业 IT 内部控制评价的工具

目前很多企业的很多业务流程都还存在人工控制的情况，这在一定程度上降

低了企业经营效率，更有可能面临企业人员舞弊的风险。

COBIT5.0 中从治理与管理 2 个维度定义了 5 个域 37 个业务流程，IT 业务流程是 COBIT 的关注的重点，在这 37 个业务流程中，COBIT 都定义了相应的 IT 目标，这 37 个业务流程包括了企业 IT 规划、构建、运行和监控全过程，企业从这些业务过程入手，明确这些过程的控制目标和风险点，就能找出企业薄弱环节进行控制。

综上所述，COBIT 框架的应用，不仅能帮助企业在发展过程中，建立 IT 治理与管理的控制体系，也能从体系的运行情况进行评估和监控。面对我国目前的相对滞后的信息化进程来说，确实为我国企业提供了指引与启示。

中国信息化监管发展历程

（锐思咨询技术法规部）

一、 引言

信息化监管的发展与国家发展，特别是与国家法制建设之间的关系是同步的。改革开放前，由于国家法治建设受到多次冲击，信息化法律法规建设相对非常落后，缺少基本的法律规范，也没有系统概念的提出。

改革开放后，政府开始认识到信息技术和信息化监管的重要性。1987 年，我国成立了国家信息中心，在中心内部专门设立了政策研究所，重点研究有关信息法规和政策问题，并整理了《信息与信息技术立法文集》、《中国信息立法环境分析及立法探讨》、《信息化进程中立法框架建议》等内部资料。但是，直到 1994 年初，中国才由国务院出台关于信息化监管的行政法规。

1994 年至今，我国发布的有关信息监管方面的主要法律法规如下：

颁布机构	颁布时间	文件名称	备注
国务院	1994 年 2 月 18 日	中华人民共和国计算机信息系统安全保护条例	
证监会	2005 年 4 月 8 日	证券期货业信息安全保障管理暂行办法	已废止
	2012 年 8 月 23 日	证券期货业信息安全保障管理办法	
公安部、国家保密局、密码局、保密委员会和国家信息化领导小组办公室	2006 年 10 月 12 日	信息安全等级保护管理办法(试行)	
银监会	2009 年 6 月 1 日	商业银行信息科技风险管理指引	
保监会	2009 年 12 月 29 日	保险公司信息化工作管理指引（试行）	
工业和信息化部	2010 年 1 月 21 日	通信网络安全防护管理办法	

二、 信息化监管发展历程

1. 国务院:《中华人民共和国计算机信息系统安全保护条例》

1994 年 2 月 18 日，国务院发布了《中华人民共和国计算机信息系统安全保护条例》（以下简称《条例》）。《条例》共分五章三十一条。第一章，总则，规定了《条例》制定的目的，即“保护计算机信息系统的安全，促进计算机的应用和发展”，并规定了信息安全保护的范围，即“重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全”。第二章，安全保护制度，规定“计算机信息系统实行安全等级保护”，同时规定对信息安全产品，如杀毒软件、防火墙、入侵检测软件等，实行销售许可制度，并对其它具体的保护措施做了进一步规定。第三章，安全监督，规定了公安机关在计算机信息系统保护工作中行使的职能。第四章，法律责任，规定了对于各种违反计算信息安全保护的行为相应的处罚措施。第五章，附则。

《中华人民共和国计算机信息系统安全保护条例》是我国专门针对信息网络安全问题制定的首部行政法规，为保护计算机信息系统的安全提供了法律保障。这部条例明确对计算机信息系统实行等级保护，同时规定对信息安全产品，如杀毒软件、防火墙、入侵检测软件等，实行销售许可制度。为了实施这一制度，公安部于 1997 年制定了《计算机信息系统安全专用产品检测和销售许可证管理办法》。2000 年 4 月 26 日，公安部又根据该条例出台了《计算机病毒防治管理办法》，详细规定计算机病毒防治产品的生产、销售许可、病毒的检测与清除等工作。

2. 公安部、国家保密局、密码局、保密委员会和国家信息化领导小组办公室:《计算机系统信息安全保护条例》

为了贯彻《计算机系统信息安全保护条例》中所提出的等级保护制度，2004 年，公安部联合国家保密局、密码局、保密委员会和国家信息化领导小组办公室发布《关于信息安全等级保护工作的实施意见》，对信息安全等级保护的基本制度框架进行了规划。2006 年 10 月 12 日，上述四部门发布《信息安全等级保护管理办法(试行)》，开始具体构建信息安全等级保护制度。《办法》分为六章二十六条。第一章，总则，规定了信息安全等级保护的目的和含义，并规定了五个等级的信息安全等级以及信息安全职能部门对信息运营单位的五个等级的监督管

理，最后规定了各个部门的职责。第二章，信息安全等级保护工作的安全管理，规定了信息系统运营单位应履行的职责，并由相关单位进行测评、备案、监督和检查。第三章，信息安全等级保护的保密管理，规定涉及国家秘密的信息系统应当确立所处信息的秘密等级，并按相关规定进行保护，并规定对于不同秘密等级的信息系统的保密检查或者系统测评工作。第四章，信息安全等级保护的密码管理，要求“国家密码管理部门对信息安全等级保护的密码实行分类分级管理”，并要求“充分运用密码技术对信息系统进行保护”，并规定了密码的检查和测评工作。第五章，法律责任，规定了违反相关规定的行为。第六章，附则。

《信息安全等级保护管理办法(试行)》具体构建信息安全等级保护制度，是我国信息安全等级保护的重要法规，它对信息安全等级保护做了详细规定，对促进信息安全保护起到重要作用。

3. 工业与信息化部:《通信网络安全防护管理办法》

2010 年 1 月 21 日，工业与信息化部通过了《通信网络安全防护管理办法》。该《办法》对加强通信网络安全管理，提高通信网络安全防护能力，保障通信网络安全畅通具有重要的意义。《办法》围绕通信网络安全防护管理工作，主要建立了如下制度：通信网络单元的分级保护制度，即“通信网络运行单位应当根据实际情况适时调整通信网络单元的划分和级别，并按照前款规定进行评审”；符合性评测制度，即“三级及三级以上通信网络单元应当每年进行一次符合性评测；二级通信网络单元应当每两年进行一次符合性评测”；安全风险评估制度，即“通信网络运行单位应当按照规定组织对通信网络单元进行安全风险评估，及时消除重大网络安全隐患”；通信网络安全防护检查制度，即电信管理机构可以采取六项措施对通信网络运行单位开展通信网络安全防护工作的情况进行检查。

4. 证监会:《证券期货业信息安全保障管理暂行办法》、《证券期货业信息安全保障管理办法》

2005 年 4 月 8 日，证监会颁布了《证券期货业信息安全保障管理暂行办法》。《办法》分为五章十八条。第一章，总则，说明了《办法》的意义以及适用单位。第二章，安全职责划分，规定了信息系统安全运营管理的责任主体单位以及各自的职责。第三章，安全目标和基本原则，规定了安全保障工作的总体目标和四项具体目标，以及信息安全保障工作应遵循的四项基本原则，即：责任制原则，规范化原则，全面统筹原则和实用性原则。第四章，安全保障要求，。办法规定：

主体单位应建立明确的信息安全组织体系、全面的信息安全管理体系以及有效的信息安全技术体系。第五章，附则。目前，该办法已废止。

为了更加适合中国证券期货信息安全保障工作的需要，2012 年 8 月 23 日，证监会通过了《证券期货业信息安全保障管理办法》。此办法分为七章五十一条。第一章，总则，规定了信息安全保障工作实行的原则，即“谁运行、谁负责，谁使用、谁负责”、安全优先、保障发展的原则，此外，办法还规定了信息系统安全运营管理的责任主体单位以及各自的职责。第二章，基本要求，规定核心机构与经营机构应当具有合格的基础设施，设置合理的网络结构，建立符合业务要求的信息系统，具有重要信息系统具有自主开发能力，防范木马、病毒等恶意代码的能力，建立完善的信息技术治理架构、管理制度和操作规程，提供多种互为备份的远程接入方式。第三章，持续保障要求，要求核心机构和经营机构应当采取各种措施持续保障信息安全。第四章，产品及服务采购要求，要求采购的产品及服务应满足的要求。 第五章，行业自律，“证券期货行业协会应当引导鼓励行业信息技术研究与创新，增强自主可控能力”，“引导供应商规范参与行业信息化与信息安全工作，促进市场公平竞争”。第六章，监督管理，证监会阻止监督管理工作，并对违反规定行为进行相应的惩罚。第七章，附则。

《证券期货业信息安全保障管理办法》保障了证券期货信息系统安全运行，加强了证券期货信息安全管理工作，促进了证券期货行业的信息安全保障工作。

5. 保监会：《保险公司信息化工作管理指引（试行）》

2009 年 12 月 29 日，中国保险监督管理委员会出台《保险公司信息化工作管理指引（试行）》。《指引》共七章四十四条。第一章，总则，规定了《指引》制定的目的和信息化工作对业务发展目标的意义。第二章，组织经营和规划，规定了信息化工作的组织结构。第三章，基础环境和信息系统建设，规定“各公司应运用信息技术加强内部控制与合规建设，促进内部控制流程与信息系统的有机结合，实现对各项业务和事项的自动控制，减少人为操控因素”。第四章，安全保障与风险控制，规定了安全保障和风险控制的原则和各项措施。第五章，发展环境。第六章，审计与备案，规定“各公司应建立信息化工作的风险评估机制和信息系统审计制度，由独立于信息技术部门的有关部门负责审计工作”，并规定定期向主管部门进行信息化报告。第七章，附则。

《保险公司信息化工作管理指引（试行）》是保险公司信息化工作的重要规章制度，对于保险公司的信息化建设和风险评估起到非常大的促进作用。

6. 银监会:《商业银行信息科技风险管理指引》

2009 年 6 月 1 日，银监会颁布了《商业银行信息科技风险管理指引》。《指引》共十一章七十六条。第一章，总则，规定了《指引》制定的目的，适用单位，信息科技、信息科技风险的定义和风险管理的目标。第二章，信息科技治理，规定了董事会应履行的信息科技的职责、首席信息官的职责以及对相关人员应采取的风险防范措施。第三章，信息科技风险管理，规定：商业银行应制定信息科技风险管理战略，应制定持续的风险识别和评估流程，实施全面的风险防范措施，应建立持续的信息科技风险计量和监测机制，并防范因监管差异而造成的风险。第四章，信息安全，规定商业银行应采取各种措施保障信息安全，包括：建立和实施信息分类和保护体系，建立有效管理用户认证和访问控制的流程，设立物理安全保护区域，根据信息安全级别，将网络划分为不同的逻辑安全域，确保所有信息系统、计算机操作系统和系统软件的安全，采取加密技术，配备切实有效的系统，制定相关制度和流程，相关人员培训等。第五到八章包括信息系统开发、测试和维护，信息科技的运行，业务的持续性以及外包。第九到十章分别为内部审计和外部审计。第十一章，附则。

《商业银行信息科技风险管理指引》对于商业银行加强信息科技风险管理提供了指导，既使商业银行从业人员各司其职，又保证商业银行采取相应的措施防范信息科技风险，保证信息安全。

三、 总结与应用

《中华人民共和国计算机信息系统安全保护条例》、《信息安全等级保护管理办法(试行)》、《通信网络安全防护管理办法》、《证券期货业信息安全保障管理暂行办法》、《证券期货业信息安全保障管理办法》、《保险公司信息化工作管理指引（试行）》、《商业银行信息科技风险管理指引》这几部法律法规是我国信息化监管的主要组成部分，公安部、文化部、教育部、证监会、保监会、银监会、中国人民银行等各个部委发布的相关通知、通告也是我国信息化监管的有机组成部分。其中，证监会、保监会、银监会出台的三部部门规章（即《证券期货业信息安全

保障管理办法》、《保险公司信息化工作管理指引（试行）》、《商业银行信息科技风险管理指引》）是当前我国金融行业信息化监管的主要规章制度，对证券公司、保险公司、商业银行的信息化监管起到促进和监督的作用。

我国信息化监管的法律体系已初步形成，相关立法已涉及到：网络监管、信息安全、电子商务等各个方面。但这些法律法规仍不足以高效地保护互联网的安全。其本身也存在一些问题。主要表现在：

第一、立法主体多、层次低、缺乏权威性。从前文所列的信息化监管法规中可以看出，除了《中华人民共和国计算机信息系统安全保护条例》属于国务院的行政法规之外，其余全部是部门规章。立法主体多、层次低是显而易见的。

第二、部门规章的数量远远大于行政法规的数量。我国的各个部、委、总局、总署都制定其职责范围内的部门规章，这些规章制度数量庞大。此外，我国还存在数量相当庞大的各类通知、通告、制度和政策之类规范性文件，这些通知、通告的法律效力不高，并无强制性措施和惩罚措施。

第三、缺乏系统性和协调性。由于我国缺乏统一的法律法规制定架构，各个部、委、总局、总署制定了数量庞大的规范文件，各个部门缺乏沟通，因此，规定之间缺乏系统性和协调性，甚至不同部门的相关规定会出现立法冲突，令众多单位无所适从。

当然，为了弥补各个部门之间协调性的问题，在国务院的领导下，我国相关部门会联合出台规章制度，例如前文提到的《信息安全等级保护管理办法(试行)》就由五个相关机构联合出台。这也是我国法规制定方面的方向。不过，缺乏统一架构使得我国的法规制度不可避免地存在冲突，因此，由国务院领导，在统一架构下制定信息化方面的法规依然是不可或缺的。

总而言之，虽然我国信息化监管的法律法规已经较为完善，但法律法规之间存在层次低、缺乏权威性、系统性和协调性的问题，这是今后我国此方面立法考虑的重中之重。

方 法 指 南

信息环境下信息系统的内控评价

（锐思咨询研发部）

一、信息系统内控评价的内涵及意义

随着信息技术的高速发展，日益进步的信息技术帮助企业经营者将先进的管理理念融入业务流程中，管理与业务流程的自动化大大提高了企业的经营效率。这也就意味着，传统手工的业务控制活动正逐渐被信息化手段的控制活动所代替。由此，随着信息化在企业经营管理中覆盖面的不断延伸，企业内部控制有效性对信息系统的依赖程度愈来愈高。企业内部信息系统的安全、可靠、有效，将在很大程度上决定了内部控制的有效性。因此，定期对企业信息系统的设计及运行开展内控评价显得尤为重要。

信息系统的内控评价需要由独立于审计对象的第三方，以客观、公正的立场，审查与评价企业内部信息系统的规划、开发、运行和维护等一系列活动，以及信息系统的运行环境等，以确定信息系统的运行是否安全、可靠、有效，信息系统得出的数据是否可靠准确。

二、信息系统内控评价的主要内容

企业开展信息系统的内控评价将主要围绕以下两大方面进行：

其一：信息系统的运行环境评价

- IT 治理。即企业应设置适当的机构，并配备相应素质的人员，明确其部门与岗位的职责、工作程序、运营管理机制和监督实务，以达到公司治理中对信息方面的要求。
- 信息系统的生命周期管理。即企业从信息系统的规划、开发/采购、测试、上线运行到日常维护与使用。
- 信息资产的保护。即通过适当的安全体系，保证信息资产的机密性与完整性，从而在一定程度上保证企业内部信息的安全。

- 灾难恢复和业务连续性计划。一旦发生突发事件，导致连续的业务被中断或破坏，灾难恢复计划可以确保灾难对业务影响最小的同时，及时恢复被中断的 IT 服务。

其二：信息系统的应用评价

- 信息系统运行的合理性。信息系统运行过程的合理性评价与传统控制活动的控制对象一直，为企业的生产经营过程。与传统控制相比，不同的是：传统控制通过纸质传递和保留信息，存在签字后补或倒签等可能，而通过信息系统可以在一定程度上规避该类行为。

三、信息系统内控评价的步骤

信息系统内控评价与一般的内控评价主要过程一样，分为准备阶段、实施阶段、报告阶段。与一般的内控评价相比，所不同的是在评价的实施阶段需要具有丰富信息技术和知识的人员参与，方能更加全面、更加彻底地对企业信息系统进行检测。各阶段的评价思路和方法主要如下：

（一）准备阶段

信息系统内控评价的准备阶段主要是为了初步了解企业信息系统的基本情况，以便于拟定合理的评价计划。准备阶段开展的主要工作列示如下：

（1）了解企业信息系统的基本情况，如企业管理信息系统及各系统权限分配的机构，各信息系统的组成、环境、运行年限等。根据了解到情况，判断是否对各系统开展评价，明确评价的难度，所需时间以及人员配备等。

（2）了解企业内部控制制度，以便更加准确、快速的确定测试的范围和重点。

（3）确定评价范围，编制评价计划。在评价计划中，需对范围、时间、人员、工作步骤以及任务分配、评价风险等方面做出安排和评估。

（二）实施阶段

实施阶段是信息系统内控评价的核心阶段，主要工作围绕准备阶段制定的评价计划进行开展。具体工作内容如下：

（1）信息系统的运行环境

- IT 治理。根据准备阶段了解的部分情况再次进行深入调研，通过访谈、符合性测试等方法，实际了解信息系统管理的各岗位设置是否合理，如是否存在不相容职责未进行有效分离等情况。
- 信息系统的生命周期管理。针对信息系统从规划到引进（开发/采购）再到上线运行及日常维护等一系列活动，通过穿行测试或符合性抽样检查等方法进行检测，了解企业引进各系统及日常维护过程中的管控程序是否到位。下面从信息系统开发及运行维护两个方面进行简要介绍：

信息系统开发：

1）是否编制开发计划，计划中是否明确描述系统的效果，计划是否制定有可行性报告等；

2）设计阶段：是否已确定用户功能和性能需求，是否确定用户的数据需求等；

3）编程阶段：是否有程序说明书，并按照说明书进行编写，编程与设计是否相符，编程的书写、变量的命名是否规范，编写过程中是否由作者或他人进行测试；

4）测试阶段：测试数据的选取是否具有代表性，用户是否参加测试，测试结果是否准确记录等。

信息系统运行维护

1）是否定期对信息系统后台进行监控，是否定期对信息系统的杀毒软件等进行更新等；

2）维护计划是否合理，维护是否经相应人员审批，是否对发现问题进行了修正，维护记录是否有文档保留，旧系统的废除是否得到授权等。

- 信息资产的保护。了解信息资产的外部运行环境（如机房的物理环境），信息资产是否能随意调配、报废、报废处置的过程等。该检测可以通过实地查看、符合性或实质性抽样等方法。
- 灾难恢复和业务连续性计划。了解企业信息系统的灾备计划，如企业是否实行双机异地热备份、定期对备份介质进行检测等。该检测可以通过访谈及实地查看了解。

（2）信息系统的应用

- 信息系统运行的合理性。针对信息系统是否被正确、合理的设计以及是否能够有效运行，可以通过采用符合性及实质性测试。测试过程与一般的内控测试相似。不同之处主要体现在数据输入、处理及输出。数据输入主要关注输入信息输入权限分配的合理性，信息输入的防错和保护措施的有效性等；数据处理主要关注数据处理的时间、差错率等；数据输出主要关注对数据的保护、保密措施是否有效，输出信息是否准确、及时等。对数据输入、处理、输出的过程进行评价，可以通过查询信息系统使用记录，并按时间顺序进行排列，然后检查信息的创建、编辑和删除都是由谁完成。

（三）报告阶段

报告阶段的主要工作有：整理检测过程中发现的证据；复核底稿，形成评价结果；编制评价报告。

四、信息系统内控评价的风险

企业虽然可以定期组织进行对信息系统的内控评价，但这过程也出现了新的风险，主要表现为以下几个方面：

（1）系统管理的人员未执行职责分离，这就给有心人留下了漏洞，这些人就可以利用职务之便故意修改、窃取秘密，同时可以在系统中篡改数据且不留下检查痕迹；

（2）系统开发或防护不善，可能遭遇外部黑客或其他电脑高手的侵入，企业内部数据将面临失窃或破坏，这也会使得信息系统的内控评价因缺少数据而无法开展；

（3）企业因未能办理双机异地备份或其他方式备份，一旦遭受灾难性事件，则可能导致企业大量信息的丢失。

企业信息系统管理的层次和关键控制点

（锐思咨询研发部）

进入 21 世纪以来，随着互联网络的普及和社会信息化事业的快速发展，信息技术也越来越多的被应用于企业的日常管理活动中。通过信息化手段，可以促进企业管理现代化，能对信息进行快速反应，更合理地协调人、财、物在生产实践中的调配，从而达到优化管理流程，有效降低成本，加快技术进步，增强企业核心竞争力的目的。

相较于传统的企业管理模式，信息技术和 IT 系统被用来进行辅助设计、辅助制造、过程控制、信息传递和辅助管理。随着信息化的普及，目前而言大部分的中小企业在内部推广单项信息技术，如 CAD、CAM、财务电算化、OA 等；小部分的大型企业已经能实现信息化在生产和管理上的覆盖率达到 80%-90%，并正努力将各单项管理系统整合成一个大的管理平台，在该平台上从事信息数据的收集、统计、分析、使用和决策。无论是在大、中、小型企业，随着信息化程度的不断加深，随之而来的信息系统管理也会给企业带来越来越大的风险。

本文主要从企业信息系统管理的层次分析开始着手，重点从管理角度来剖析信息系统管理中存在的主要风险及其关键控制环节。根据信息系统的来源不同，可以分为直接采购、自行开发、共同开发等；根据系统存在风险的原因不同，可以分为两类：一是系统本身的设计需要保证不存在缺陷或系统漏洞；二是通过控制措施防范系统管理和操作人员的失误或故意违法犯罪行为；根据系统引进或开发的先后顺序可以分为前、中、后期。

一、企业信息系统风险管理的层次

1、系统设计管理

大多数的企业会通过信息系统的直接采购或设计外包来实现单项信息系统的上线实施，少数企业会自行研发和设计部分信息系统。但无论采用哪一种方式来完成信息系统的上线，就系统设计本身均存在以下风险：

（1）系统引进或开发前期

1）企业在引进系统时缺乏统筹规划，各部门仅在需要时提出申请，由企业相关部门组织实施系统采购或开发，可能带来的风险如下：

□ 造成信息孤岛。各个系统各自为政、孤立存在，削弱了信息系统的协同效用，甚至引发系统冲突。

□ 重复建设。各个系统存在内部部分功能的重复建设，给系统操作人员带来不便的同时也在一定程度上造成人力、财力的浪费。

2）未进行充分调研，并未对操作流程或管理流程进行梳理和优化，即实施系统采购或程序设计，可能会带来的风险如下：

□ 不适用。上线后的系统流程不能完全与企业实际的操作模式或管理程序相匹配，该系统最终不得不被抛弃或重新设计。

□ 系统设计缺陷。在系统流程中可能存在设计缺陷，不仅不能带来效率的提高，反而给企业带来经营和管理风险。

3）供应商的选择不恰当，未能根据企业的实际需求内容或项目特点找寻有类似项目特长、经验和资质的供应商，可能带来的风险如下：

□ 不能很好提供或开发适合企业实际需求的系统。该供应商不一定能很好的理解企业的需求，提供的系统可能无法满足企业全部系统或无法与其他系统进行较好的对接。

□ 后续服务跟不上。系统勉强上线后，系统的更新与维护的支持能力不足，缺乏有效的保障。

（2）系统引进或开发中期

1）需求本身不合理，对信息系统提出的功能、性能、安全性等方面的要求不符合业务处理和风险防控的需要，可能带来的风险如下：

□ 系统设计出现漏洞。购买人员或系统开发人员如不能在过程中及时发现这些不合理或不完善的地方，直接导致系统在设计上出现漏洞，影响后期的使用，

更为严重将为公司管理留下风险的隐患。

□ 对于计划直接采购系统的企业而言，可能找不到与不当需求相匹配的产品。

2）技术上不可行或成本效益倒挂钩，可能带来的风险如下：

□ 无法开发出相应的信息系统，在技术层面就无法完成企业的需求目标。

□ 开发成本过大，给企业带来的便利或效益却不足以抵消该成本，从成本效益配比原则来看，不合理。

3）提供的设计方案不能完全满足用户需求，或没有考虑系统建成后对企业内部控制的影响，可能带来的风险如下：

□ 设计方案不全面，将会导致后续系统的变更频繁，在一定程度上增加企业的资金成本或其他成本。

□ 系统运行后衍生新的风险。从风险防控角度来看，反而通过系统的设定将风险固化或扩大，也给系统管理人员或有心人留下来可趁之机。

4）程序编制结果及设计不符，缺乏有效的程序版本控制，可能带来的风险如下：

□ 与实际需求不符。程序编制的偏差将直接导致系统设计在功能、性能、易用性等方面与实际需求不符。

□ 重复修改。在企业自行开发设计系统过程中，各程序员编成风格差异较大，程序可读性差，会导致重复修改或修改不一致，延滞项目周期的同时也造成了成本的浪费。

5）采用系统设计外包，缺乏外包跟踪评价机制或跟踪不到位，可能带来的风险如下：

□ 质量较差。系统设计外包，企业不能时时掌握供应商的编制情况，无法保证供应商在人员选用、质量把关方面是否存在疏忽的地方，及时了解系统设计每一阶段的实际情况，将直接影响系统的质量。

□ 进度把控较难。设计过程的主动权在供应商，若缺乏定期跟踪督促的机制，将无法保证系统能在规定时间内完成。

6）缺乏可行的上线计划，或上线培训做的不到位，可能带来的风险如下：

□ 无法系统性发现运行问题或设计漏洞。上线进行信息系统测试，缺乏可行的上线计划，将会导致测试过程中可能存在疏漏，无法全面、系统的排查设计漏洞。

□ 系统上线测试的培训做的不到位，涉及的系统使用人员可能无法很好的使用系统，进而也无法保证系统测试的顺利进行。

（3）系统引进或开发后期

没有建立规范的信息系统日常运行管理规范，缺乏对系统的例行检查，可能带来的风险如下：

□ 前期未发现的漏洞依然存在于系统当中，导致一些人为恶意攻击系统，给企业造成严重的损失。

□ 常见的系统故障未能得到及时的排查，长时间的累计可能给系统带来更大的安全隐患。

2、系统应用管理

(1)系统管理人员或操作人员控制

1）系统日常管理、维护和监督的过程中，存在“三员”职责未能进行有效分离，该“三员”分别为系统管理员、安全员、审计员，可能带来的风险如下：

□ 无法做到相互独立、相互制约，增大了系统保密和安全风险。

□ 三员中的某一员的权限过大，让其能够了解企业更多的经营信息或系统漏洞，可能会让其利用所得到的信息或漏洞，进行舞弊行为。

2）企业未建立严格的系统变更申请、审批、执行、测试流程，可能带来的后果如下：

□ 系统管理人员随意变更系统设置，影响企业系统运行的稳定、持续和信

息安全。

□ 申请、审批等未留下书面痕迹，无法有力的保证问题的可追溯性，也不利于系统可持续的维护管理。

3）对信息系统程序的缺陷或漏洞防护不够，对计算机病毒清理不及时，可能带来的风险如下：

□ 导致黑客的攻击，造成企业信息泄露，给企业的信息安全带来防范的严重风险。

□ 病毒清理不及时，可能导致系统运行不稳定甚至导致系统瘫痪。

4）对于系统数据的录入、复核、编辑等操作动作未能通过职责分离、权限分配等方式进行有效控制，可能带来的风险如下：

□ 系统内数据的不准确、不完整、不及时，将导致数据输出或使用结果的错误，进而影响经营决策的判断。

5）敏感或关键信息被非授权用户获取，或数据输出过程中被篡改，可能带来的风险如下：

□ 信息泄露。敏感或关键信息被竞争对手或其他有心人所得，将可能给企业带来无法估量的损失。

6）信息系统未能定期备份，或对备份的系统进行定期检测，可能带来的风险如下：

□ 企业信息系统在损坏后无法恢复，从而造成重大损失。

(2)硬件设备控制

1）硬件设备分布物理范围广、设备种类繁多，可能带来的风险如下：

□ 设备安全管理难度大。

□ 导致设备管理人员或其他成本的增多，安全防范风险增大。

2）机房的物理环境不合格，或机房的进出管理不严格，可能带来的风险如

下：

□ 设备的使用寿命缩短。

□ 影响企业的信息资产和信息保密安全。

二、信息系统的关键控制点

以上对信息系统开发和日常管理过程中可能存在的一些主要风险进行了分析，下面主要讨论从系统引入到日常管理中的关键控制点。

（1）企业应对信息系统的引进或开发做全盘的统筹，信息系统的建设是个投资巨大、历时很长的工程项目，规划不好不仅自身造成损失，由此而引起企业运行不好的间接损失更为可观。在信息系统规划的过程中，首先要站在企业发展战略规划的高度制定管理系统信息化的目标，只有目标明确了方能决定项目成本预算和实施周期等。

（2）企业应在某一信息系统实际需求时，首先应根据系统需求的内容、项目预算、实施周期、市场成熟产品的特征等多方面共同考虑和评估，决定项目引进的方式：直接采购，设计外包或者共同开发。

（3）企业在决定系统引进方式之后，需要进行充分的调研了解，对系统管理中可能涉及的业务或管理流程进行详细梳理和优化，同时根据各层级人员的需求及项目大小选择合适的供应商。

（4）在供应商确定完毕后，需在合同上对项目、进度、赔款等关键要素进行重点关组，防止不利于企业的条款让供应商有漏洞可钻。

（5）若采用设计外包方式进行引进，企业应组建专门的小组负责与供应商进行定期或不定期的沟通，将企业的需求准确的传递给供应商，并对整个项目的质量和进度进行跟踪评价。若采用共同开发，需将双方的职责内容划分明晰，同时需将知识产权等在事前进行明确。

（6）上线前需制定较为周密和详细的上线测试计划，应区分单元测试、组装测试（集成测试）、系统测试、验收测试等不同测试类型，建立严格的测试工作流程，提高最终用户在测试工作中的参与程度，改进测试用例的编写质量，加

强测试分析，尽量采用自动测试工具提高测试工作的质量和效率。具备条件的企业，应当组织独立于开发建设项目组的专业机构对开发完成的信息系统进行验收测试，确保在功能、性能、控制要求和安全性等方面符合开发需求。

（7）对于已上线的信息系统，应加强对系统使用人员的培训，使之对系统的操作步骤更加熟悉，同时应定期收集系统使用人员的系统使用情况反馈，以便于系统的更新或二次开发。

（8）加强对信息系统的日常管理和运行维护。系统管理员、系统安全员以及系统审计员应做到“三员”分离，相互监督和制衡，对于三者的职责和每日的工作内容进行明晰；对于机房的物理环境包括温度、湿度、电源、防火系统等需按照相关国家规定进行维护；对信息系统需进行定期的备份，并注意加强备份的介质的保管，对其能否使用进行定期测试。

浅谈数据信息化在企业管理中的应用

（锐思咨询研发部）

一、引言

目前，企业信息化的建设已经被越来越多的企业所关注，通过信息化技术，企业能够在战略决策、经营效率以及风险防范方面都做出正确的判断和合理的优化。相较于传统的数据收集手段，信息化手段的应用能够在很大的程度上解决诸如样本量选取较小、特殊数据抓取困难等问题，节省了大量的工作量、降低了大量的人工成本。随着企业信息化不断的完善和优化，还能帮助企业的管理者进行一定的战略决策。

笔者结合日常咨询项目的最佳实践，通过本文简述企业信息化在管理中的应用，希望能给予企业管理有一定的启示。

二、传统信息收集所遇到的问题

传统的信息收集方式中，现场抽样是一种比较常见的方式，通过抽取一定样本量的证据凭证，来识别样本中存在的问题，从而发现缺陷。但是在这一过程中，就会产生如下一些问题：

1.样本量的选取较少

在某个业务环节几万个样本中，由于是人工来进行测试工作，只选取了其中一部分样本量，这样就难以发现该业务环节所存在的缺陷，或者是难以准确的体现该环节的缺陷重要程度。

2.样本多为已经发生的事项

多数情况下，测试过程中所选取的样本，多为过去所发生的业务，相对应的，企业的内部控制所采取的控制措施也是针对这一过去所发生的事项，并未对该事项未来将有的发展趋势做出预测，从而可能对决策造成不必要的偏差。

3.特殊数据监控不力

企业的授权审批体系，规定了不同层级的负责人所能够签署的合同，如采购合同会规定不同金额的合同由不同层级的人来签署。而有些合同在订立时，合同

金额设定低于审批的临界值，也将给企业内部控制带来隐患。

综合以上所述，这些问题都可能使企业对自身经营管理的判断和完善产生些许偏差或遗漏。

三、企业信息化架构

那么针对以上可能存在的问题，企业的运营要做到合规且高效，笔者认为，企业有必要利用信息化的数据分析与统计，来对企业的经营情况做出评价或是企业的发展趋势做出预测。

如何来建立一个以数据为基础，通过数据分析来帮助企业完善日常运营和帮助战略决策呢？结合日常咨询项目，笔者认为可以以下图体系为参考，以信息系统为依托，建立企业信息化数据分析架构。（如图1所示）

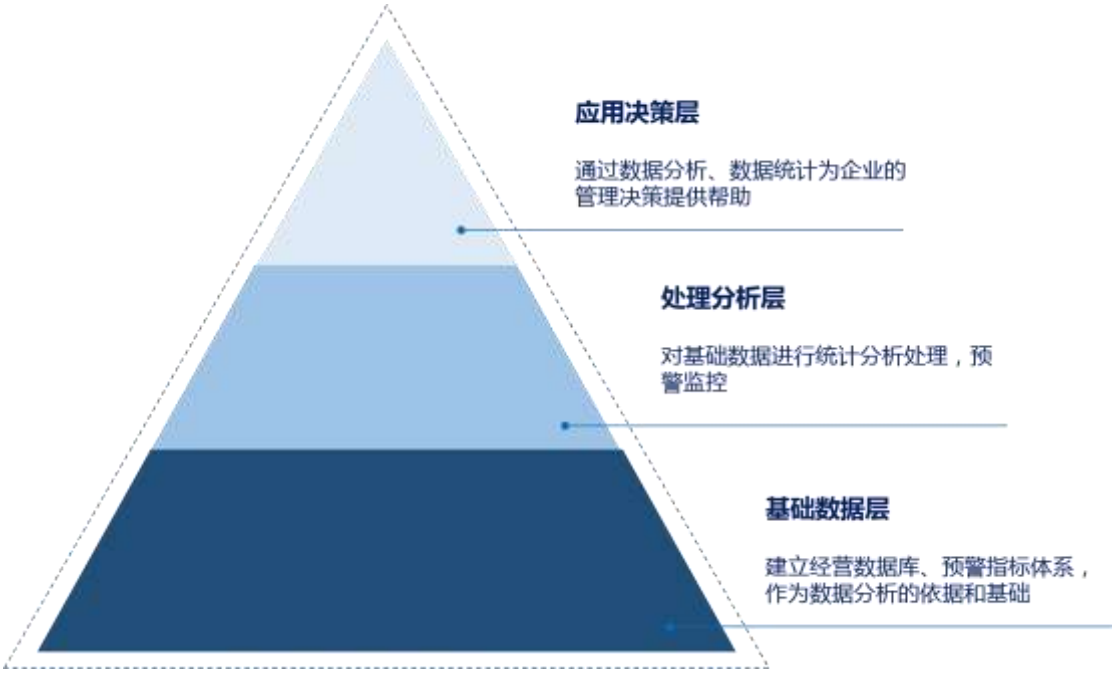


图1 企业信息化数据分析架构

如上图所示，企业信息化数据分析架构主要有三个方面：基础数据层、处理分析层以及应用决策层，以下分别进行阐述：

1.基础数据层

实现基础数据库的功能，将企业各个业务环节所会产生的经营数据录入系统，并确定数据指标作为预警体系的标准。在这一层中，经过数据的采集，利用信息系统建立起基础的后台数据库，作为数据处理分析的基础。那么，对数据就提出了以下要求：

1）采集的数据是否完整。数据分析是针对分析对象的基础数据，采集的基础数据是否完整，有无异常都会影响分析的准确性。通过系统进行数据样本的采集，也可避免人工不能完整采集数据的情况。

2）采集的数据是否真实。数据分析的对象是企业经营过程中真实发生的业务、流程、记录等，运用数据来反映这些真实发生的事项，对数据本身也要求了其真实性，这直接影响到数据分析结果的真实性。

3）采集的数据是否全面。企业的经营管理是多方面的，在《企业内部控制基本规范》配套指引中，对企业十八个业务循环进行了规范，数据是否能全面地反映企业的经营管理状况，也是影响分析结果的重要因素之一。另外，在这一点中，还应该注意数据之间的相关程度，在企业中，不同部门的不同业务之间，具有一定的相关性，所以采集的数据还应该注重数据之间的关联性。

2.处理分析层

经过数据的采集，在这一层中，需要将数据进行统计分析，获得能够为企业管理带来收益的效果。也就是说，企业要将基础数据层的数据转换为有效的信息来服务于企业管理。那么就对统计分析做出了要求：

1）要能够明确会发生什么事情——笔者认为，这是数据分析中较为重要的关键问题，即数据的分析能够合理的预测企业未来的发展趋势，明确企业的竞争优势和劣势，从而帮助高层管理人员在企业战略发展上做出更好的决策。

2）要能够分析为什么会发生——通过对数据的分析和监测，寻找数据背后所反映的事实，分析其中原因，从而改善企业内部的关键流程，降低风险与舞弊事件的发生。在这一点上，所关注的重点是企业的内部控制，数据能够准确的反映企业内部尚需完善的流程。

3.应用决策层

在这一层中，就是对数据的综合运用，数据的存在形式不仅仅在数据库中，而是通过不同形式为企业的管理进行服务，这里就需要将需要企业建立信息化平台，将数据分析的结果分享到各个层级中去。那么综合的信息化平台能为企业带来什么呢？

1）一个管理者进行管理决策的平台

数据的收集可以涵盖包括市场的信息，竞争对手的信息，在这样一个大数据

的平台下，企业管理者可以通过数据的横向对标，比较自身企业在行业之中的优势与劣势，明确企业的定位，那么就能更加具有针对性的加强企业的竞争优势，创造收益。

例如，某企业在日常运营中需要进行原材料采购，通过数据分析发现，2012年企业全年的采购平均价为300元/吨，而市场的平均价格在200元/吨浮动，在一般情况下，就能明显看出该企业原材料采购的议价能力较低，给企业增加了不必要采购成本。

2）一个优化风险的内部控制平台

数据的收集同时也涵盖了企业内部的数据收集，通过对企业各部门的数据监测，能够很清晰的反映企业各部门流程管理情况，企业可以设置一定的数据指标，来达到异常监控预警的功能，来帮助审计部门发现风险，控制风险。

例如，在合同管理方面，合同倒签是企业普遍存在的现象。企业可以通过信息系统，对合同的审批日期和签订日期进行监控，检测是否存在签订日期早于审批日期的情况，发现异常可以及时进行核实，以达到优化风险的功能。

3）一个高效的数据收集平台

前文已经提到，传统的数据收集手段会带来许多问题，导致数据分析的结果可能会产生偏差和遗漏，那么以这样一个偏差的分析结果所做出的战略决策必然会存在风险。而信息化的数据收集平台，就能在很大程度上解决这样的问题。

例如，对于特殊数据的抓取——还是以采购流程为例——如果采购员与供应商签订的合同金额故意低于某个审批临界值，从而避开企业制度规定的审批层级，就很容易给舞弊创造环境。通过信息化的手段，后台实时对如采购合同金额进行监控，就能有效的控制这一问题的发生。

他 山 之 石

COSO 基于云计算的企业风险管理

（COSO）

在计算机技术日益进化时代中，信息处理从大型机转到了个人电脑在到以服务器为中心的计算在达到互联网。如今，许多企业正认真考虑采用云计算——下一个技术和商业合作的主要里程碑。更加有效的在互联网上提供托管服务，云计算可能使企业能够增加他们的商业模式的能力和满足计算资源需求，同时避免重大基础设施、培训、人员和软件的投资。

在 2010 年秋季,谷歌高管作证的美国国会一个小组委员会表示,全球有三百万多家企业客户正在使用云服务。Gartner inc .预测，云计算将会在 2014 年成为一个价值 1400 亿美元的行业。

系统虚拟化、系统资源管理和互联网的技术进步已导致了云计算成为一种能迎合众多类型企业技术需求的可替代方式，其有以下好处：

- 瞬时计算资源履行；
- 标准化一般技术平台；
- 以更低的成本最大化技术支出；
- 减少内部技术支持人员的需要。

当然对于任何新机会，云计算也需要承担相应的风险。它让企业之间产生一个不同维度的协作和人员之间的相互作用，新的组织依赖性，更快的资源履行和新的商业模式。

在美国 Treadway 委员会 COSO 企业风险管理——整体框架中，是一个为企业建立共同的语言和基础来整体评估和监督风险的文件。引用该文件中的一个观点：“企业风险管理能够使企业管理能有效地处理风险和机会的不确定性，以及加强企业创造价值的能力。”云计算可以对操作环境产生巨大变化；COSO 企业风险管理——整体框架的使用将可以促进企业风险识别和战略制定以及云计算所面临的机会和不确定性。

这本刊物意图是利用 COSO 的原则的企业风险管理——整体框架，来提供一种能识别细微风险的指引以及云计算对于企业的影响。企业高管对于云计算的风险和益处了解的越多，他们就能更加有效的管理企业。这里给出的指导将使高管通过使用云计算来识别、监控并缓解或接受风险。

1.什么是云计算？

定义

云计算是一个计算资源分配和采购的模型，其使得企业能够从任何地点通过因特网连接获得计算机资源和应用程序。根据企业对于云解决模型的使用，便将使部分或全部的企业硬件、软件和数据不再只停留在其自己的技术基础设施中，相反，所有这些资源都会位于一个与其他企业共享的技术中心中，并由第三方运营商管理。

云计算专业术语

- **云服务供应商（CSP）——**第三方供应商，通过云计算提供应用程序交付、托管、监控和其他服务。根据所需的云解决方案，一个企业可以与多个供应商建立合同。

- **多用户共享——**对于大多数云技术解决方案来说，客户就是众多共享资源和技术的租户里的其中一个。多租户的概念就是如何分配和提供资源给客户。例如,一个云计算客户的数据可能被安置在一个大型数据存储平台，这个平台也能与其他有类似云计算方案的租户使用。

云分配模型

引用美国国家标准技术研究所的云计算分配模型最常见的类型的是：

- **私人云——**专为单个企业建立，并由第三方企业运营和管理；其设施可以建立在企业内部。
- **社区云——**由几个企业共享或者基于某种特定的共同利益建立起来（例如：任务、行业合作或法规遵循需求）。它可能是由行业组织或者第三方管理，该设施也能建立在企业的内部。
- **公共云——**提供给普通公众或大型工业集团，建立于云服务提供商。
- **混合云——**由两个或两个以上的云（私有，社区或公共）组成，其保持独特的实体，同时通过规范化的或专有技术绑定在一起，使得数据和应用程序产生可移植性。

云服务交付模型

云服务供应商提供的云解决方案通常被称为云服务交付模型，最常见的是：

- **软件服务（SaaS）**——应用程序组用来实现特定的功能或流程(例如，电子邮件、客户管理系统、企业资源计划系统和电子表格)。一个更进化的被称为业务流程服务(BPaaS)的软件服务正越来越受到欢迎。利用 BPaaS，整个业务流程(例如，工资和供应链管理)都外包给第三方提供方并由其综合云服务方案提供支持。
- **平台服务（PaaS）**——开发环境来构建和部署应用程序。供应商为客户提供可以在其基础设施上操作系统和程序的专有平台。
- **设施服务（IaaS）**——供应商提供一个完整的资源虚拟数据中心 (例如,网络,计算资源和存储资源)。

2.机遇

适用于几乎所有形式的云计算的一些机会和潜在收益包括以下几点：

- **成本低廉**——云客户只需支付计算资源的使用,而不是购买或租赁那种并不能在所有时间都能充分发挥作用的设备。如果云计算是用来满足所有的技术需求，企业将不会有物理空间需求和为维护专用的数据中心来承受的设备成本。企业从云服务供应商处获得所有计算资源费用可记为支出(即,获得美国的税收减免)。而这种税收收益通常并不能从内部专用的数据中心获得（资本支出和摊销因素所决定）。
- **分配速度**——计算资源方面，云服务提供商可以比内部 IT 部门更快满足需要 (例如,服务器处理和数据存储)。完成计算或程序的时间可以从几个月的时间缩小到几周，或者从几周缩小到几天，甚至在几小时内完成。
- **弹性和技术资源适应性**——一个企业可以在没有资本支出的情况下从一个服务器到若干个服务器向上和向下扩展其容量。在没有多余能力在高需求阶段获取计算资源时，这种能力能使得企业可以获取大量计算资源来面对临时的集中需求。
- **减轻技术管理**——设置和运营 IT 部门是成本高昂且耗费时间的。云

计算给予企业集中更多的时间在其核心目标。大多数的云服务都是基于一个能够促进更好支持的预先构建的标准化基础技术。这个基础技术也使供应计算资源更容易,反过来有利于更一致的技术升级和加快实现资源请求。

- **环境效益**——如果每个企业用云计算来替换其私有数据中心,其结果将极大减轻整体功耗、碳排放，和物理土地的使用。

3.风险

在 2004 年 COSO 企业风险管理——整体框架中定义:“风险是发生某种事件并产生与目标相反效果的可能性。”

风险的类型(例如,安全性、完整性、可用性和性能)在云技术和非云技术解决方案里是相同的。如果云解决方案被采用，一个企业的风险水平和风险状况将在大多数情况下改变 (取决于方法和用途)。这也与供应商协议中规定的风险事件发生可能性和影响力的大小有关。

一些典型的云计算风险包括:

- **破坏性的力量**——对于某些企业，促进创新（增加速度）和成本方面的云计算本身是可以被视为风险事件的。通过降低新竞争者的行业进入壁垒，云计算可能会威胁到或破坏一些商业模式，甚至使其淘汰。例如，流媒体在互联网是一个技术解决方案，明显降低了 CD 和 DVD 在物理零售商店的销售和需要。现有的竞争对手充分利用云技术也许能让其在市场上的前进步伐带来新的思想和创新。由于减少了资本支出，云计算解决方案带来可观的短期成本节约。对比不使用云技术的竞争对手来说，一个企业采用云技术可以获取更高的利润。因此，当一个行业企业采用云解决方案，那么该行业其他组织可能被迫效仿采用云计算。

- **与供应商和同一云租户处于同一生态风险**——当一个企业采用第三方管理云解决方案，那么在法律责任，风险范畴，事件升级，事件响应和其他领域等与供应商产生依赖关系。供应商的行为和其他云租户可以以各种不同的方式影响企业。包括以下几点:

（1）在法律上,第三方云服务提供商和企业客户是不同的企业。然而，如果

供应商忽略或不承担责任，企业客户应相应承担法律责任。但如果企业客户不承担责任，那么供应商并不会牵扯到法律责任。

（2）云服务提供商和企业客户可能有单独的企业风险管理方案以应对他们各自领域的潜在风险。只有在少数情况下(涉及非常高成本合同)，供应商会与其客户一起整合部分的企业风险管理项目。使用第三方云计算的企业所要面对的风险范畴是服务供应商所正在面对的所有个体公司各自的风险的总和(将在第 5 部分"了解企云计算中的企业风险管理"中进一步讨论)。

- **缺乏透明度——**供应商不太可能透露其流程、操作、控制和方法的详细信息。例如，数据存储的地点，供应商所使用和分配资源的算法，云计算架构中安全组件的具体控制或者客户数据是怎样在云技术中相互隔离的，企业客户对此了解相当少。

- **可靠性和性能问题——**系统故障是一个风险事件，可以发生在任何计算机，特别对云计算将构成特殊的挑战。尽管服务水平协议可构造，以满足特定的需求。但如果一个租户或事件对云基础设施有意想不到的资源需求，供应商便可能有时无法满足性能要求。

- **供应商缺乏应用程序的可移植性和互操作性——**许多供应商以其云技术来提供和开发应用软件。这些工具是专用的，它们可能只能在特定的解决方案体系结构创建应用程序。因此,这些新应用程序(由这些专有工具创建)可能不适合系统框架外的云解决方案。此外，应用程序开发的专用工具和企业在一个特有供应商存储的数据越多，更换供应商就变得更加困难。

- **安全性和遵从性问题——**流程云计算的支持，安全性和保留问题可能出现相关的法律法规,比如 2002 年的萨班斯-奥克斯利法案(SOX)，1996 年的健康保险携带和责任法案(HIPAA)，以及不同国家出台的各种各样的数据隐私保护政策。数据隐私和保护的法律将包括爱国者法案,欧盟数据保护指令，2010 年的马来西亚个人数据保护法案以及印度的 IT 修订案。在云技术中，数据是企业直接控制

之外的。根据云解决方案 (SaaS、PaaS,或 IaaS)，一个云技术企业客户可能无法获取并查看网络运营或安全事件日志，其掌控在供应商手中。供应商可能都没有义务披露这一信息或可能无法在不违反与其他租户签订的保密协议而实现这种做法。

- **高价值的网络攻击目标**——供应商对于多个企业的整合运营比单个企业更具有价值吸引力，从而增加攻击的可能性。因此，在供应商提供的云技术中，保密和数据的完整性所存在的固有风险是相对较高的。

- **数据泄漏风险**——企业用户和应用程序共享资源的多租户云环境中，呈现出了一种数据泄漏风险，而这种风险当企业使用专用服务器和资源时是不存在的。这种风险体现出的一个关注点：数据隐私和机密性要求。

- **IT 部门的变化**——如果云计算在很大程度上被采用，企业在基础设施管理、技术部署、应用程序开发和维护方面不需要过多的 IT 人员。这对于余下的 IT 人员的士气和奉献精神都存在打击。

- **云服务提供商生存能力**——许多云服务提供商是相对年轻的公司，或者云计算业务对于经营良好的公司是一个比较新的领域。因此，云服务的预期寿命和盈利能力都是未知的。在公开时,一些供应商缩减他们的云服务，因为他们不能盈利。云计算服务提供商可能最终被整合。因此，客户可能面临运作中断或承担的时间和费用来寻找一种替代解决方案，如转换回内部托管的解决方案。

除了这些风险,云计算的某些特征可能会导致其他不那么明显的挑战 (这些不明显的点将在第 7 节其他考虑因素中谈到)。

在整个企业风险管理中，对于拥有较小的前期资本投资的一些管理团队来说，可能愿意承担其企业在公共云服务中的风险。初创企业和风险资本家都倾向于集中投资业务模型，而不是一个当投资失败时仅有的不具价值的技术基础设施。相比以前的技术模式，初创的公司可以通过云技术来让企业发展的更迅速更具有效

益。

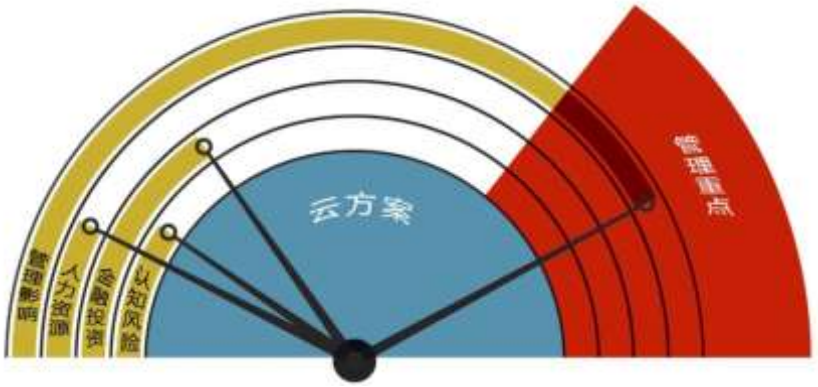
所有在这里讨论的云计算风险应该认真考虑(即接受风险评估)，这些风险一旦成为现实将造成很难看的结果，这里的很多风险不太可能通过与供应商之间的合同条款来减轻 (很多合同甚至是协商的，但很多商品云服务不是)。因此，可能需要目前供应商提供的云技术方案之外的解决方案来解决。

4.云计算的商业操作环境中的变化

企业应当意识到云计算对其企业风险管理的操作环境和账户的风险和其他影响。在某些情况下,云计算能很容易进入到一个企业并绕开典型的管理监督控制。当一个组织投入大量资源的努力，这可能需要数月甚至数年才能完成，从而使传统工艺和控制方面需要管理的参与和批准。这种高投入很可能吸引在风险评估、审计和监督委员会的高级管理层的注意力。

当资金投入较少或人员需求较少时，一些云解决方案可以在短时间内迅速采用，并同时指需要较少的资金投入和人员需求。一般来说，大型投资等于大影响，但对于云计算是不同的，一个小的投资可能会有更大的影响。需要花费大量的精力来分析可能与直觉相反的云计算风险和执行相关的尽职调查。因此，管理可以忽视执行耗时的步骤，例如确认符合法律或法规的要求或评估供应商在组织业务和风险状况的潜在影响。图 4.1 表明通过云计算，很多典型的控制点（例如人力资源和财政）并不需要达到高层来监督的水平。

图 4.1 云方案的采用来省去高层的监督

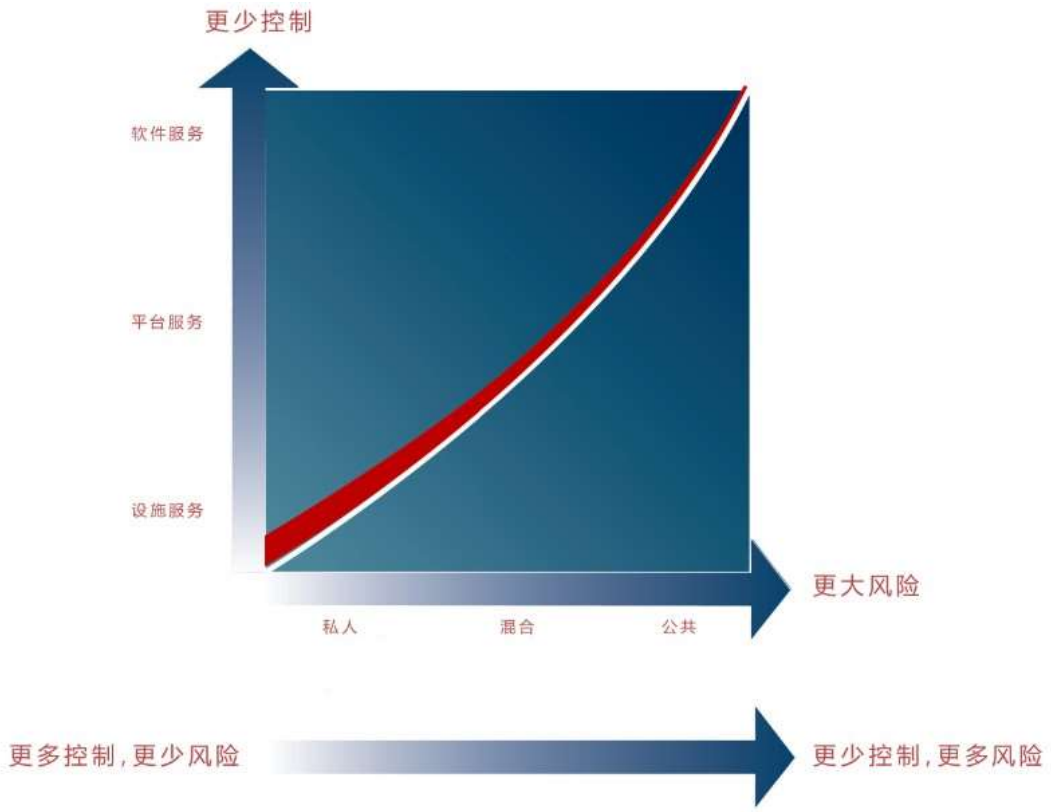


最重要的是,管理层也懂得,通过大多数云解决方案(除了内部私有人员)企业将会拥有更少的对解决方案的直接控制，当然也不可避免的提高了内部风险。

例如，一个软件服务（SaaS）的企业的控制方案已经将自己部分或全部 IT 功能，包括 IT 控制，转向了第三方提供商。图 4.2 说明了企业放弃的和保留的控制的程度，完全这同时也取决于云服务的交付类型和分配模型。

具体来说，最大程度的控制和最小内在风险与设施服务（IaaS）方案有关。相比之下，使用软件服务方案（SaaS）,该企业保持最少的控制权力，而必须接受最高水平的内在风险。在任何情况下，管理者应根据可接受的风险水平来评估云分配和交付模式，因为这将决定首选类型的云计算环境和相关的必要的控制。

图 4.2 云服务分配模型与交付模型和内在风险的关系



5.了解云计算中的企业风险管理

云计算的到来，应被视为企业风险管理操作环境的一项内容。

不管多少努力，只要提前确定目标和方式将会提高成功的机会。因此，一个定义明确的企业目标和具体的云计算职责的计划将使管理做出合理的决策。一些

企业风险管理的先决条件应该被考虑进一个有质量是云计算计划，并且最终的云解决方案，是一个强有力的治理模型,一个健全的报告结构,一个准确对内部

IT 技能和能力的理解和一个确定的风险偏好。

一些管理团队觉得风险评估和治理项目是可选的。企业采用云解决方案而没有应用正式风险评估或花费任何努力调整其 ERM 或者治理计划是很常见的。在采用云解决方案之前的最初阶段（策略已经明确）纳入云治理是一个最佳方式。对于那些已经采用云解决方案但没有遵循最佳方案的企业来说，仍须谨慎执行风险评估和建立云治理。

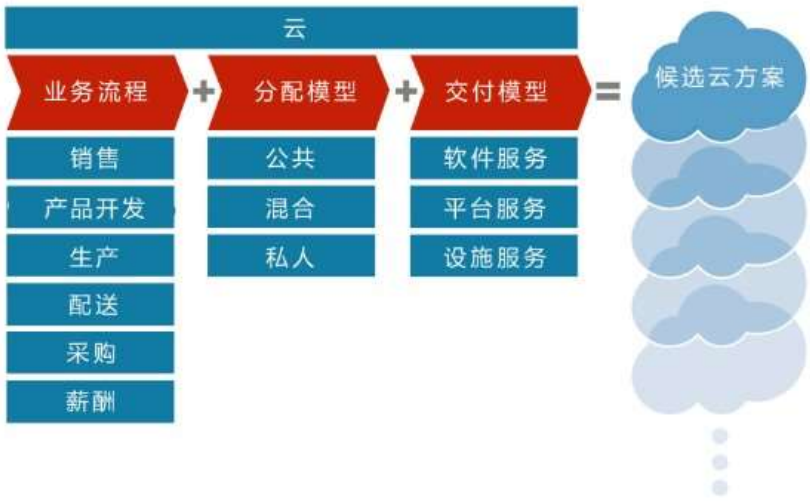
利用 COSO 框架建立云计算治理方案

企业现有的云计算范例中的风险管理项目的调整程度极大地取决于云所支持的业务流程，分配模型，服务交付模型和与供应商订立的风险和控制环境的本质。

在许多云方案下，企业不再对技术和技术相关的管理过程有完整的或直接的控制。管理上必须确定对于给定云解决方案是否有对整个范畴内潜在事件的风险偏好，因为有些事件超出了企业传统管理的范围或者对企业服务供应商有所影响的事件。

图 5.1 描述了通过云支持业务流程,分配模型和服务交付模型，具体的云候选方案是如何派生出不同的选项的

图 5.1 云方案的产生

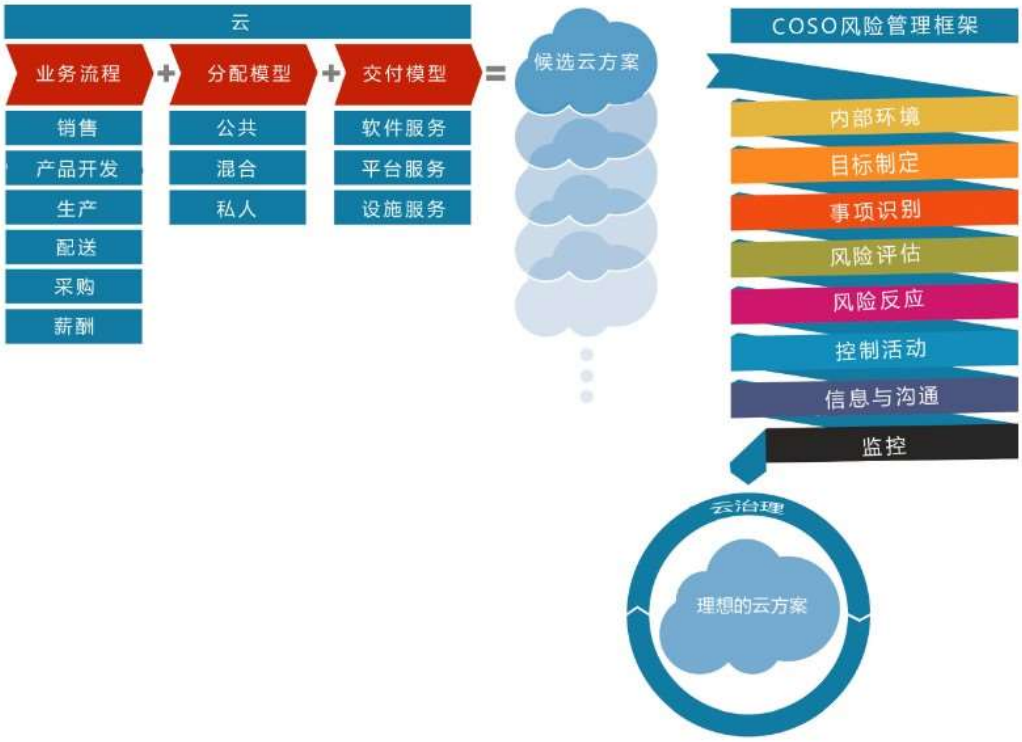


采用云计算对企业来说可能是一个重大的改变，企业管理能够使用已被证明的企业风险管理框架来有效地评估和管理相关风险。COSO 框架提出的企业风险

管理——整体框架已经建立了一个共同的语言和基础，其用来建立一个有效的云治理结构来专门适应一个给定的云解决方案。

最初的 COSO 框架是介绍一个 ERM 多维数据集。图 5.2 中，这个框架展示了为了了解将会给到企业的候选解决方案的各自的优缺点，每个 ERM 组成部分组成的路径(从内部环境)。当候选方案中，每个流程都完成时，理想的云解决方案将会连同其相关的云治理的建立而出现。

图 5.2 将 COSO 风险管理框架运用到云方案



在云解决方案已经被实现的情况下，COSO 企业风险管理框架可以通过确保所有的主要方面的程序(例如,目标、风险评估和应对风险)已经解决了管理需求来建立、完善或者执行云治理计划的质量保证检查。有效的云治理项目也可以通过云方案的实施来应用于 COSO 企业风险管理框架。

最佳的情况是，管理使用 COSO 企业风险管理框架来确定适合管理风险偏好的云解决方案的配置选项(例如,业务流程,分配模型和服务交付模型)。通过候选云方案模型管理在 COSO 企业风险管理框架中的评估，可以简明地标识适应每个云解决方案场景(如风险将分为各个选项的组合)所需的相关风险和风险缓解策略。这个评估将使管理者在云解决方案实施前，选择其理想云解决方案和创造一个深思熟虑的云治理项目做出谨慎的风险管理和治理决策。

这部分其余阐述了通过COSO企业风险管理框架的各个组成部分评估云方案的几个重要点：

内部环境——内部环境是企业就如何看待风险和控制的基础和企业风险偏好的定位。例如,如果管理的政策是不外包任何操作(例如,风险规避的文化)，这一政策将会限制云分配方案可行的选择和服务交付模型，并使得私有云解决方案可能是唯一可接受的替代方法。

目标制定——管理人员需要评估云计算是如何符合企业目标的。根据不同的情况，云计算可能会为企业提供一个契机，使其增大实现目标的能力，或者提供获得竞争优势的机会，但这需要新的目标来定义。

事项识别——公司管理层需要负责识别可以影响目标完成的事件(机遇和风险)。当一个企业雇佣供应商时，事件识别和风险评估过程的复杂性将会增加

企业应该把外部环境因素（监管、经济、自然、政治、社会和技术)以及内部因素(文化、人力和财政健康)考虑到风险识别和评估流程中去。使用公共或混合云解决方案，管理层也需要将供应商对外部环境和内部环境的影响考虑进去。管理层应该致力于完善企业的案例库，因为预期事件对风险评估过程的性质和质量有着巨大的影响。

风险评估——管理人员应该结合云策略评估风险事件来确定每个云计算选择风险的潜在影响。理想情况下，风险评估应该在企业使用云方案之前完成。

云计算可以影响以下几个风险评估的关键点：

- **风险范围**——一个企业的风险范围包括了其整个需要管理的风险整体。当采用云解决方案,一个企业的风险状况取决于风险的可能性、风险的潜在影响以及供应商风险范畴的整合（参阅本节末的“供应商与其他租户对风险范围的影响”)。
- **固有和剩余风险**——企业必须评估其固有风险事件，然后做出应对和确定残余风险。不同的企业，不采用云方案的固有风险和残余风险比采用云方案的企业可能高也可能低。

- **可能性和影响**——当云方案被采用时，某些事件发生的可能性和相关的潜在影响在许多情况下都会变化。是否能够准确地确定风险取决于企业是否有一个全面、准确、当前的风险案例库。

在某些情况下，管理者并不能访问与供应商控制环境相关的信息。因此，必须做出某些假设来完成风险评估。

风险反应——一旦有关云计算的风险被识别以及对于企业目标已经评估，管理人员需要确定其风险应对。有四种类型的风险应对：

- 回避——退出引起风险的活动 (即不适用云计算的或只考虑私有云类型的解决方案)。
- 减少——实施控制活动和采取行动来减少风险的可能性，影响，或两者兼具。
- 分担——通过转移或其他方式分担部分风险来降低风险发生可能性和影响 (例如,购买保险)。
- 接纳——不采取行动来影响风险可能性和影响。例如,当一个企业没有能力对供应商进行直接管理，这个企业只能接受较高的固有风险水平。

对于大多数混合云或公共云解决方案，管理者依赖于第三方管理控制;这降低了企业直接降低风险的能力。这意味着采用供应商解决方案会使固有风险水平增加，因此管理者可能需要增加其风险偏好。

由于风险应对在云计算中起到了重要作用，将在第 6 节“推荐的云计算风险应对”进行进一步讨论。

控制活动——传统类型的控制活动——预防、侦测、手动、自动和实体化——也适用于云计算。引进云计算的区别是，一些控制责任可能保留在企业而某些控制责任将转移到供应商。

如果企业现有控制或的水平是中等或者较差的，采用云解决方案可能会加剧内部控制的弱点。例如，如果一个企业密码控制或数据安全较差而将其计算环境迁移到一个公共或混合云解决方案，外部安全漏洞可能会大大增加，因为现在访

问企业技术权限的基础是通过公用网络的。

信息与沟通——为了有效地运营业务和管理相关风险，管理依赖于对内部和外部事件的各种资源及时和准确的信息沟通。通过云计算,从供应商获取的信息可能没有内部 IT 系统那么及时和准确。因此，实现管理的信息和通信需求可能需要额外的或不同的信息处理流程和来源。

管理也应该监督与供应商相关的外部信息(例如,财务报告,公开披露,提交给监管机构的文件显示,行业期刊，还有的其他公告的云计算租户)，对某些供应商和其租户的影响同时也可能影响到自己企业。

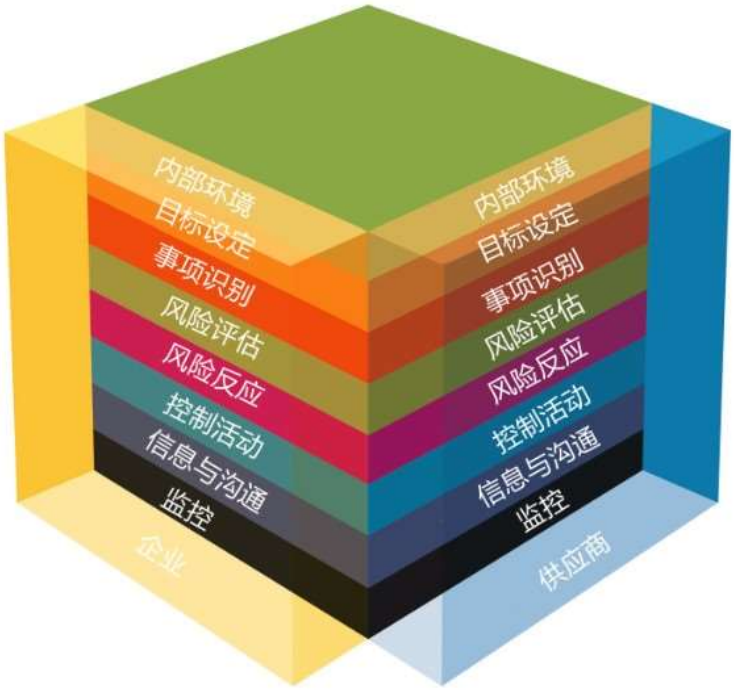
监控——“风险应对,曾经有效可能变得无关紧要；控制活动可能会变得不那么有效，或不再执行，或实体目标可能会改变。“2004 年发表的 COSO 企业风险管理——整体框架，在云计算时代仍然是可用的。管理必须持续监控企业风险管理程序的有效性，来确保程序足以充分满足相关风险需要并促进实现组织的目标。有效的 ERM 程序是进化和动态的，并且必须加快云方案的进化来应对竞争对手的云方案和法规变化。

鉴于云计算的潜在和实际的影响，整个企业的高级管理人员(不限于首席信息官)需要通过职责分配来实现云计算治理。(“附录:云计算管理——角色和职责”提供了关键云计算职责的范例)

对供应商和云租户风险状况的影响

企业从专用的内部计算环境转移到公共云或混合云计算解决方案是将企业风险控制程序范畴转化成其自身与供应商相结合的形式。图 5.3 描述了这个概念。

图 5.3 企业与供应商相结合的风险控制体系



该企业的数据和流程保留在与其他云租户共享的数据环境中。这种行为以及供应商和其他租户发生的事件可能会直接影响到自身企业。由于供应商的风险暴露能影响云的客户，这些风险必须纳入到供应商提供的解决方案中的风险范畴中去。这种混合的环境中可能会改变企业的风险状况,因此需要新的不同的控制程序。这种风险范畴的结合也可能延伸到那些共享同一设施资源的云租户企业。

作为云风险评估过程的一部分，管理者需要考虑与其他租户相关信息的风险，例如,他们的身份,他们的应用程序分配以及他们成为网络攻击目标的可能性。

因此，管理层的风险管理程序应该解决自身风险管理程序以及伴随着的供应商的风险管理程序。管理需要识别可能会影响自己企业和那些可能影响供应商及其租户的风险和事件。

6. 推荐的云计算风险应对

随着云计算的到来，无论管理的意见或加入云计算的决定，每个企业的运营环境日新月异。管理人员应该适应企业风险管理项目和相应的控制。以下部分阐述了对某些公开出来的重要的与云相关风险的应对。

风险—未经授权的云活动

风险应对—云的政策和控制

无论管理立场是否冒险进入云计算，所有企业都应该有政策建立管制，以防止和检测未经授权的采购和云服务。由于低成本的云服务启动相对传统技术收购中，当前控制程序比如支出限制可能不会引起管理层的注意。

例如，某大型企业下的一个业务部门决定利用 CRM 系统进行新产品的首次销售。没有建立企业云政策，业务部门在开始销售的时候可能没有通知 IT 部门或者指定资本费用预算。(云解决方案只需要互联网接入和信用卡)。系统一旦运行，将会充满客户的信息。因此，机密客户信息将存储在不受企业控制的外部环境中。

对于决定采用云计算的企业来说，以下是就未经授权的云活动的一些建议的风险应对：

- 建立一个明确的业务流程和管理层认为适当的数据处理云使用政策；
- 创建或更新购买云计算服务权限的政策；
- 认证过的云服务供应商；
- 定义供应商服务策略以及管理层与供应商之间的沟通机制。

风险——缺乏透明度

应对——供应商控制环境评估

当需要的信息是不完整或者很难获取时，完成一个对供应商高质量、全面的风险评估是很困难的。在大多数情况下，供应商的内部控制环境对客户是不可能完全可见的。

例如，变更管理控制如用户验收测试和生产和开发环境的隔离通常是用来确保应用程序系统的质量。对于公共或者混合云软件服务解决方案，云客户企业对

供应商管理控制变更不能直接控制或详细了解。因此，云客户的SaaS 解决方案可能需要增强或改变他们的流程来测试应用程序更改，当然这也取决于他们的风险偏好和供应商的企业服务控制(SOC)报告(假设供应商已经产生SOC 报告的费用)。

为了能部分克服了解供应商操作控制这一挑战，管理层应该在调查时进行控制活动的询问以及进行相关尽职调查。管理层也应该与供应商在合同条款中写明相关的审计权限。作为评估供应商内部环境的一部分，管理层应该(最好在与供应商签约前)调查供应商时如何解决某些风险事件的。为进一步了解供应商内部控制环境和云解决方案的风险和质量，管理层可以进行内部审计来评估或可以要求独立的审计报告比如由美国注册会计师协会学院(AICPA)出具的审核业务标准16(SSAE16)和服务组织控制 2(SOC 2)的报告，其内容涵盖了安全性、可用性、处理完整性、机密性和隐私。

风险——安全、合规、数据泄漏和数据管辖权

应对——数据分类策略和流程

转用公共或混合云计算解决方案可以改变当前数据存储的位置、事务处理和控制结构。这些变化要求进行相关分析，因为他们可能影响企业业务是否仍然符合适用的法律和法规。合同条款应该明确定义满足对于企业和法规需要的供应商行为。

如果一个企业数据采用云方案管理(除了私人云)，而没有能力去识别数据的特定的当前位置(服务器或存储设备)或数据的历史地点的。(注意，很少部分的供应商会提供指定数据存储国家的服务)。这个位置的挑战是由于多租户云环境中云客户的资源重用和动态分配的性质所造成的。这种无法识别特定地点以及数据存储地点的云服务可能会在满足探索或数据传递存在障碍。这种限制可能会严重影响数据存储或(程度较轻)当企业需要云计算支持的事务处理活动。

有关客户数据存储位置(例如,国内或国际)的供应商合同条款应该是根据数据保护条款来确定和评估。一些商品 CSPs 可能不揭示它们的位置，但会分享一些关于司法管辖区的信息，因为他们必须遵守法律。在企业将数据转移到第三方组织之前，管理人员应理解监管含义和法律管辖的责任，作为一种谨慎的预防措施。比如,一个美国供应商将数据存储在德国，这 CSP 必须符合德国的数据保护

法律，欧盟数据保护和通知的法律，也受美国爱国者法案的要求。遵从性和数据管辖权对企业来说并不是新概念；然而,从事云加深了在这些领域方面的检查义务。

当一个企业在使用一个公共或混合云分配模型时，无法精确地控制数据存储位置，但可以控制存储在云的数据类型。从风险管理的角度来看，企业使用公共或者混合云解决方案，有效的数据分类规范和流程是比较关键的。

数据分类政策应该清晰地定义敏感信息并禁止企业以外的组织直接控制。作为结果，分类政策应该确保数据分类的目的，所有权和敏感性在整个企业中明确的进行了沟通和理解。

数据分类过程应该包括以下几点：

- 法律、监管、知识产权和安全性的要求的各种类型的数据;
- 确定各种类型的数据敏感性(公共、限制或高度敏感);
- 建立数据传输需求(如加密)
- 确定数据所有者——拥有决定数据访问权力的人员(例如,业务经理或合规人员)

风险——透明度和放弃直接控制

应对——管理监督和监测操作控制

在非外包的情况下，管理者可以对企业内部控制环境采取直接控制行为。在公共或混合云模型下，管理者转移部分或完全直接控制权给供应商。在大多数情况下，供应商主要从一种宏观的角度为其客户提供稳定和安全的平台来满足客户的控制需求。供应商的解决方案不可能满足每个客户的独特需要。管理者评估供应商的云方案以及实施控制活动是必不可少的职责以便供应商的方案能满足企业的所有要求。

管理人员应该对本身放弃而给予供应商的控制活动有明确的认识，因为这种认识将确定管理人员进行相关监控活动。对于上市公司，对于那些放弃的控制活动而影响到财务报表应该实施预防措施。使用云计算并不意味着管理层可以不用担心。

维护控制环境的组织的云解决方案可能是管理者和供应商共同的责任。供应商的第三方审计报告(如 SOC 报告)包括一个定义供应商对其客户的责任的被审计

单位的互补性控制，从而明确排除供应商的控制责任。因此,管理层必须确保被审计单位的互补性控制融入企业控制环境。在某些情况下，如复杂性增加情况下，供应商可能会将一部分职责转移到另外一个供应商。如果是这样的情况，所有供应商的审计都应包括在 SOC 报告中以便企业对外包业务有完整的了解。最理想的情况是，为了在现实中避免这种复杂的情况，与供应商订立合同时就禁止一切形式的分包。

一个使用混合的或公共的云计算解决方案的企业应该验证供应商的控制活动来确保他们时结合管理风险偏好的。企业还应该定期验证供应商的控制有效性。在所选择的云服务交付模型基础上，企业与供应商的共同的责任是在方案实施，技术操作和访问管理上的共同控制。

风险——可靠性、性能、高价值的网络攻击的目标

应对——事件管理

企业需要评估除了其自身对于系统死机和数据被盗等方面的突发事件反应流程外，其供应商突发事件反应能力。

供应商的系统故障或安全漏洞可能会影响多个客户。当这些类型的事件发生时，其 CSP 的最主要的焦点在于解决云环境的问题；也就是说,供应商不大可能专注于解决每个单独租户的问题。因此,管理的事故响应计划不应该仅仅依靠其供应商，除非管理是愿意在突发事件发生时接受最坏的情形。

下面的例子阐述了其固有的风险及系统死机或者网络攻击时的缓解控制：

系统死机——系统死机可以发生在任何的计算环境。在发生灾难性故障，同时需要满足多用户需求时，低优先级的企业可能并不能从供应商那边享受到需要的服务。

能缓解系统死机的控制程序

- 聘用其他具有与首选供应商有相同解决方案的供应商或者对数据进行备份。
- 对系统实时监控
- 实现自动化工具使得资源需求可以从其他供应商处获得
- 审查服务协议来确保供应商能在系统死机时提供完整服务。

网络攻击——每个企业都存在被网络攻击的固有风险。对于大型企业数据整

合的供应商设施给予了黑客较大的目标去攻击。考虑这样一种情况，一个与大型企业共享云服务基础设施的小公司，其被网络攻击的可能性被大型公司拉升到同一种水平。

可以缓解被网络攻击时的控制程序：

- 只将不必要和非敏感的数据存储在第三方供应商处；
- 对托管在云服务上的数据进行加密；
- 利用其他供应商的方案或者自身内部控制来进行故障转移策略。

一个不太明显的情况可能是企业如果使用公共云方案，在发生风险事件时，可能会将企业暴露给公众或被媒体宣传。例如，如果一个著名的云服务供应商(例如,亚马逊和谷歌)遇到了网络攻击而服务中断或发生安全漏洞，很快就会被宣传出去。供应商可能不能马上就影响到的企业，发生原因，恢复时间或者事件影响做出立即答复。然而，供应商对其客户的声誉已经遭到破坏，即使供应商的操作方法并未被影响到。

风险——不遵守规定

应对——对外部环境的监控

管理人员需要监视会影响自身的运营和供应商运营的外部环境的变化。法规以及电信供应商的变化对云方案的如何实施有很大的影响。

法规主要的变化主要是在数据私密性方面。各个国家对其公民的个人信息会实施保护限制措施。因此，基于云方案的数据存储可能要存储在特定的国家，而不是供应商任选的存储地。

风险——厂商锁定

应对——准备退出策略

企业使用供应商的方案越多或者其需要供应商支持的运营越多，就更加依赖供应商。没有什么是永恒的，更改供应商或者放弃云服务对于管理者都应该是审慎的。因此，管理人员应该研究一个退出策略或者应急策略作为云方案策略的一部分。

风险——不符合披露要求

应对——财务报告披露

新的要求可能是对于依靠供应商的关键流程进行披露。按照云解决方案在业务运营或者其他风险的潜在影响，上市公司必须意识到信息披露是作为合规和公开透明的一部分。

7.云计算委员会的监督、管理决策以及其他一些因素

云计算委员会

考虑到云计算提供的机会的巨大潜力和风险影响，云计算应该作为企业整体活动被考虑进去，以及应该在董事会时讨论相关事宜。

下面是一个企业的董事会进行治理监督的一些问题：

- 管理层对于考虑采用云计算达到什么水平，管理人员在其中的位置是怎么样的？
- 谁负责整理与云计算相关的业务风险？
- 竞争对手在进行怎么样的云方案？
- 企业管理是否有有效的流程去监督云计算的采用？
- 云计算对企业整个内部控制结构有怎样的影响(改进,不变,或减少)？
- 企业是否对云计算的复杂性有足够的理解？
- 云计算是否符合企业风险偏好？
- 在于云供应商订立合同和从事阶段是否进行了尽职调查(需要监测过程)？
- 是否已经订立了期望的供应商最小服务水平？
- 依靠第三方供应商是否减少了企业管理风险？
- 如果云计算被用来帮助企业，其风险是否确或者向投资者披露？

云计算管理决策

决定是否采用云计算需要管理者评估内部环境——包括业务操作、流程标准化，IT 成本和积压的 IT 项目——加上外部环境——包括法律、法规及竞争对手采纳的云计算。

作为管理考虑云计算的定位和策略，它应该解决一些关键性问题,包括:

- 企业对于管理外包的看法？
- 企业是否快速增长而需要

云方案？

- 企业是否处于一个成熟的市场，而需要使用云计算为节约成本以保持竞争力？
- 企业的运营功能和流程是否足够成熟和规范来让企业采用这一平台？
- 企业现有的 IT 功能和成熟度？
- 企业应如何准备采用云计算？
- 云计算是否能用来获得收益，或者规避风险如数据泄漏等？
- 谁应该参与评估过程和作出决定？
- 采用云服务，企业如何在业务运营环境中充分管理风险？

采用云服务，企业如何在业务运营环境中充分管理风险？

在决定再用云服务的诸多因素包括业务支持流程，具体的分配模型，具体服务交付模和特定的供应商可能的服务提供商都应该考虑。

应该指出的是,在发布时，许多供应商提供的是商品式的服务方式以及签订一刀切的协议和服务协议，而不是以企业各自的方式。

与其他商业决策相比，如进行一个投资回报率分析、所有权的总成本分析,和潜在供应商的尽职调查——加上开始一个试点项目——都是需要谨慎的行为。

其他因素

在做出任何云决策时，以下是一些额外的和不明显值得认真考虑的方面 (因为他们可能会增加风险或者引起新的风险):

- 云解决方案的定价可预见性——许多供应商采用的是现收现付定价模型,这使得计算云服务的成本显得简单。然而,能够决定若干年投资回报率的是以云计算历史价格趋势为基础的计算。例如，管理者可以预测云解决方案的价格在未来会上涨还是下跌？当前价格的云计算方案能有效多久？是不是物价上涨的上限规定的合同？
- 忠实租户——企业与一个供应商合作的越久,企业就对供应商系统处理和数据存储需求更加依赖(这不可避免地会随着时间的推移而增长)。随着时间推移，供应商转换成本或者回归内部自己管理的成本会一直增加。在某些情况下供应商也意识到当企业内部控制技术人员解散或者供应商对重要业务流程有强大支持的时候，企业将成为忠实的租户。那么，价格的上升也是可以预见的。
- 跨企业部门代表——由于云计算的潜力影响许多领域(如技术、法规遵从性,IT 员工和业务操作)、参与法律、内部审计、IT、和业务流程的人员应该参与制定采用云计算的决策。
- 企业与供应商之间明确的责任和联系——作为企业风险管理计划的一部分，管理人员需要意识到由于供应商的参与，潜在的控制问题,法律问题,业务操作问题,或者 IT 问题都可能发生。企业以及供应商的责任应从以下几个问题来确定(相关信息参阅“附录:云计算管理——角色和职责”):
  - 企业或供应商谁负责云方案的合规性？

- 企业里谁负责鼓励供应商关系和监督供应商的服务水平是否符合协议？
- 企业中谁负责保管供应商协议
- 企业或供应商谁将负责设计、管理和给予最后批准控制与安全、变更管理和访问权限相关的云计算解决方案？
- 由于企业是数据的最终所有方，谁负责在供应商管理下，管理用户和数据？
- 用户使用云计算将得到怎么样的支持？
- 用户应该直接向内部 IT 部门还是向供应商反映问题？

- 评估业务连续性需求——供应商在发生灾难事件时恢复操作的能力应该接受评估，合同条款也应该清楚地说明如果这样一个事件应该发生，供应商的义务和赔偿责任。
- 放弃特定技术领域的直接控制——保留在技术架构的控制量取决于选择的云服务交付模型。图 7.1 说明当比较自我管理和自有设施与各种云服务交付模型时，企业保留特定技术组件的程度(如应用程序系统中,虚拟机环境、服务器和存储)。

图 7.1 不同云方案交付模型的控制水平

- 最终的法律职责——通过运用公众的或者混合式云服务，管理层实际上已经分配任务给第三方，但是没有转移他对风险控制和影响数据事务处理的职责。特别地，有了公众的或者混合式云发展模型，企业是基础设施，软件，解决方案

和相关运营支持的外包组成部分。在大多数案子中，一份合同可以转移给第三方责任和义务的数量是有限的。

关于数据管辖权的法律不确定性

一个企业可能受到多层合法的管辖，取决于企业驻留在哪，云服务基础设施份额地理位置，数据从哪里收集。本文发布的时候，很明显地存在关于如何使云计算模型符合国际法了吧和监管环境。除此以外，如 HIPAA 法规，国家和区域的数据隐私发和管辖范围和其他部门进一步复杂了使用公共和混合云解决方案。

作为云计算管理和企业风险管理项目，管理层应该和法律顾问商量去决定风险相关性和遵守适用法律要求如果云计算解决方案支持一些或者所有企业的进行过程。一些云计算合法方面应该被考虑到：

- 在哪些国家需要数据储存，当供应商方法在运用的过程中？
- 什么合法管辖权是数据和系统的目标？是多样化管辖权吗？
- 如果在一个国家的供应商数据存储不同于该国家的企业和企业的顾客，法律影响是什么，以及什么是企业的合法权力，如果一个外国法院传审企业或者其客户的数据？
- 是否一个法律授权传票的企业供应商数据或者租户基础层数据企业数据可以从从一个被查收数据中被分开和孤立？
- 什么税收管辖权管理发生的事物处理？
- 如果执法机构接受了供应商的服务器在合法管辖中，它包括了企业客户不同法律管辖的数据，企业会被发现对客户违法法律权益（和相关保护法数据）对公众的客户记录和在第一时间的混合云解决方案？

8．结论

在 20 世纪最后的 10 年里，在一些圈子里已经声称云计算有和英特网带来的一样多的潜在性对企业带来的改变。适时地，云计算将建立他的标签在历史演变，科技改革的进程中。

可接受云计算是与在过去十年里普及和其他接纳趋势保持一致的（例如：社交网络和虚拟零售业），人员和设备不能被理解但是很大程度促进交流，存储信

息和商业处理。

几十年前，电脑主机被锁定在展览中心，高级管理层倍感自豪第在办公时间展示精心设计的物理安全措施，很大的数据中心和被运用到的大量的设备。来自于那个时代的高管们感到很有信心全体企业的信息资产储存在可以在戒备森严的设施中被方便验证的，如今，随着大多数可用的云解决方案，这一代人的后继高管有许多实惠的技术选项可用在他们既不能对设备做巡回展示（在许多情况下），也没有确切的企业信息资产的位置。

一些独特的关于云计算的方面可以对企业风险管理项目形成新的挑战。当风险突然出现，看似简单的采用云计算掩盖管理层变得多么复杂。然而也不能天真的认为云计算能使企业避免的了任何企业都可能降临的不利的事件—如犯罪活动、人为错误和不可预见的意外与破坏。一个有效的云治理方案是高度依赖于准确的风险理解及结合预期的风险缓解或承兑策略。通过利用 COSO 的企业风险管理框架， 管理人员将会有有效和一致的方式识别出每一个云计算的机遇和决策所需要的特定风险与应对。

使用云方案时，若没有适当的照顾，尽职调查与控制，势必会造成不可预见的问题。适当的使用—和必要的预防实施与控制到位，加上审核应用的 COSO 企业风险管理框架—云计算可能会产生众多的好处，一些至今还闻所未闻和尚未被发现的发现。在意识到云计算所带来的风险与其他问题下，高管们更能容易的实现企业的目标，因为他们的风险管理在这个动态变化的环境，可能会成为未来流行的计算模型。

附录：云计算管理—角色和责任

职位	职责
董事会成员	意识到云计算的趋势，理解管理层的观点关于影响云对产业和他的商业模型影响。
	明白监督变化的 IT 项目比如云服务
	了解管理层如何平衡风险与云效益，作为其商业和技术战略的一部分
	利用内部审计资源来保证云计划与企业风险偏好和控制哲学保持一致性

职位	职责
首席执行官	定义企业的观点和相关政策外包
	了解云计算对企业行业的影响
	了解企业是如何，在哪里运用云计算的
财务总监	提供新的披露关于云在财务报告上的使用情况
	通过云计算评估和监测总成本和投资回报率
	评估税收和云计算与选择的收益
	实施政策和控制采购的云服务政策
	监控每一个第三方供应商财务健康情况
首席法律官	确保企业的云活动室遵照法律和规章的
	监控新法律法规会影响企业解决方案或者是他的供应商，建立合规性计划
	审查和批准云服务采购政策
	提供输入数据分类策略和流程
	回顾供应商合同和保证企业利益和权利
	理解企业运营法律管辖方面，使用云托管于不同的国家
首席信息官	了解和监控云计算的潜力去支持当前业务战略和新商业机遇
	建立整体战略，并利用云解决方案
	促进有着目前 IT 基础设施的集成云解决方案进入云企业
	协助合并云管理进入企业的 ERM 项目
	实现数据分类方案综合数据所有者
	建立云资源配饰过程，用户访问管理和变更管理
	建立企业的云时间管理程序
	监控和执行供应商服务水平协议
	供应商的监视活动和其他基础层客户
首席审计执行官或内部审计师	执行定期审查评估设计的有效性和混合控制环境在控制流程被共享与供应商中

职位	职责
	运用依靠的企业的审计供应商或审查 SOC 报告以验证供应商的有效性控制
	执行定期的合规审计数据驻留在外部云数据，运用数据划分政策以此来分类合规性
	审计供应商支付和合规合同
	评估云管理

案 例 解 读

黑客帝国：挪威电信之痛

（锐思咨询研发部）

案例回放：

挪威最大的电信运营商 Telenor 在全球有 31,000 名员工，从电信运营中每年产生 180 亿美元收入，大部分在欧洲和亚洲，这使得它成为世界领先的电信公司之一，尤其是在移动业务领域。

2013 年 3 月 17 日， Telenor 首次向挪威国家警察局 Kripos 报道一例严重的黑客案，高科技间谍设法入侵了 Telenor 的安全网络并窃取了公司高管们的个人电脑信息。公司和其他电脑黑客受害者往往不愿公开报道攻击或者去警察局投诉。然而，Telenor 公司的新攻击显然是令人不安的和有潜在的威胁，所以公司周五选择去警察局报案，Telenor 同时通知了挪威国家安全机构（NSM)。

Telenor 有一个比较大的部门致力于安全，有 20 名全职员工监控公司和互联网之间的流量，公司在挪威的安全运营中心从几个 Telenor 的高管处注意到有异常的 Internet 流量时发现黑客的，当监控系统发现从 Telenor 高管的电脑经过几个国家到未知的 IP 地址的异常流量时，引起了安全人员的注意。据报道，黑客从感染的高管电脑中窃取大量的电子邮件、文件、密码和其他个人数据。

Telenor 还没有发现被攻击的高管目标，但是据报道，在高管收到这种 ZIP 形式的文件后，一旦打开，就在电脑上安装了隐藏的”木马“，一些高管收到链接到 web 地址的邮件，有几个邮件似乎来自信任的姓名和地址的联系人，甚至来自 Telenor 的同事。

Telenor 公司的安全总监 Rune Dyrlie 说 Telenor 还不能确定间谍的实际目标是什么，通常他们下载各种不同的信息来掩盖他们真正需要的。因此不能确定背后的人是谁，或者确切需要的信息。

当被问及为什么连 Telenor，拥有这么多的资源和专业人员也成为这次黑客案的受害者时， Dyrlie 强调这次攻击被迅速发现并成功的阻止了进一步的犯罪活动，他说 Telenor 已经采取预防措施来阻止同类攻击。

案例评述：

公司高管收到经过伪装的邮件并受到危害，这是一种典型的社会工程学攻击。社会工程学（Social Engineering）是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段。

通过挪威电信运营商 Telenor 的这个案例，我们可以发现很多企业在信息安全方面存在较多的薄弱之处，信息风险主要体现在以下几个方面：

首先是信息安全意识风险。在很多企业中，还存在使用弱密码、甚至空密码，密码贴在便签上的现象；个人电脑一直打开，从来不锁屏；对重要的信息不去加密，从不备份……。在由中国互联网络信息中心（CNNIC）发布的《2012 年中国网民信息安全状况研究报告》显示，中国网民只是简单地被灌输了要“重视信息安全”，但并不知道信息安全事件的危害，不知道为什么要重视，在诸如社会工程学的攻击面前也很脆弱。人是最薄弱的环节，无论拥有最好的技术、防火墙、入侵检测系统和生物鉴别设备，一个毫无戒心的人就可能使一切安全措施形同虚设。由于员工缺少相关的安全意识和培训，毫无防范意识的阅读似乎来自可信人员的邮件并打开木马附件，也就给黑客或者别有用心的人制造了可乘之机，各种钓鱼、木马邮件横行。在本案例中，也就出现了高管们的这一幕。

其次是信息安全技术风险。对很多安全产品和技术来说，主要针对已知的威胁和攻击，而对很多未知的威胁和攻击的侦测和防御能力较弱，特别是这种有针对性的攻击和精心设计的木马程序。信息安全重在预防，预防措施越到位，损失就越小，但成本也更高。案例中的针对高管的这种使用木马邮件的攻击，就其形式和技术而言，也屡见不鲜，高科技公司的互相竞争时有耳闻。专业的安全产品和技术一般对邮件的发件人地址、发件人 IP、收件人数量、收件人地址、主题和正文关键字、附件进行过滤分析，从技术防范角度看，安全产品的选择、策略的配置以及日常更新方面，可能还需要进一步提高。同时高管的电脑也可考虑部署防信息泄密终端，即使信息被窃取也难以打开，并留下痕迹。

最后是信息安全制度风险。安全界有句名言是“三分技术、七分管理”，技术有很多的成本、也影响着效率，达到的效果有限。在公司的制度中应明确规定相关的信息安全保密制度，比如不要打开来历不明的邮件附件，对重要的文件必须

加密等。企业可以参考国际标准 ISO 27001，在安全策略、安全组织、访问安全、密码、物理安全建立一整套的安全管理制度。

企业的信息化程度越高，企业对信息技术越依赖，信息系统给企业的持续运营和信誉等带来的风险也越大，企业信息安全的重要性也愈加突出。企业应定期对自身的信息安全现状进行评估，对信息资产的重要性和风险进行分级，按照风险收益原则采取一系列的管理和技术措施来应对信息安全风险。

某大型电器集团 ERP 之殇

（锐思咨询研发部）

案例回放：

1998 年初，某大型电器集团采用 Symix 公司现更名 Frontstep 公司的产品来实施 ERP。

集团上 ERP 希望能解决三个方面的问题：第一方面是是希望通过 ERP 规范业务流程;第二方面是希望信息的收集整理更通畅;第三方面是通过这种形式，使产品成本的计算更准确。

ERP 选型时，集团接触过包括 SAP、Symix、浪潮通软、利玛等国内外 ERP 厂商。开始集团想用 SAP 的产品，但是 SAP 的出价是 200 万美元：软件费 100 万美元,实施服务费 100 万美元。而当时集团上 ERP 的预算只有 500 万元人民币。国外 ERP 软件用不起，集团并没有把目光转向国内软件企业。因为在考察了浪潮和利玛等几家国内厂商之后，集团觉得国内软件厂商的设计思路和自己企业开发设计软件已实现的功能相差不大。挑来挑去，集团最终选择了 Symix，一家面向中型企业的美国管理软件厂商。集团当时的产值是 15 亿元，与美国的中小型企业相当，而 Symix 在中小型企业做得不错，价位也比较适中。而且按照一般的做法，签单的时候，一般企业的付款方式是分三笔：5：3：2 模式。而 Symix 开出的条件非常优惠：分 7 步付款的方式。双方就这样成交了。

从 1998 年初签单，到同年 7 月份，集团实施 ERP 的进展都很顺利。包括数据整理、业务流程重组，以及物料清单的建立都很顺利。厂商的售后服务工作也还算到位，基本完成了产品的知识转移。另外，在培养集团自己的二次开发队伍方面也做了一定的工作。如果这样发展下去，或许集团会成为国内成功实施 ERP 企业的典范。然而，计划赶不上变化。

到了 1998 年 8 月份，集团内部为了适应市场变化，开始发生重大的机构调整。原来，集团没有成立企业内部事业部，而是以各个分厂的形式存在。而各个分厂在激烈的市场竞争中，出现了这样的怪现象：集团自己制造的零部件，比如每个螺钉在公司内部的采购价格是 5 分钱，在市场上却 3 分钱就可以拿到。这样

必须进行大调整。

大调整的结果是将这些零部件分厂按照模拟法人的模式来进行运作。集团的想法是给这些零部件厂商两到三年的时间，如果还生存不下去，再考虑其他办法。如工人下岗、企业转产、倒闭等。

实施 ERP 在先，公司结构大调整在后。但是集团高层在调整的过程中，更多地是关注企业的生存，企业经营的合理化和利润最大化，显然没有认真考虑结构调整对 ERP 项目的影响。

企业经营结构变了，而当时所用的 ERP 软件流程却已经定死了，Symix 厂商也似乎无能为力，想不出很好的解决方案。于是集团不得不与 Symix 公司友好协商，项目暂停，虽然已经运行了 5 个月，但是继续运行显然已经失去了意义。Symix 的 ERP 现在只是在集团一些分公司的某一些功能上还在运行。

案例评述：

该集团是一个国内早期上线 ERP 失败的典型案例，但是它所暴露出的问题却是普遍性的，到现在还有很多的借鉴意义。从以上案例中，可以看到该集团的 ERP 实施，存在如下的缺陷：

首先是软件实施的规划风险。企业上线 ERP 是一个复杂的管理项目，是一项系统工程，需要有良好的规划实施方法论。在实施 ERP 前应进行管理诊断和业务流程重组，公司结构进行了大调整，业务流程重组应该提前进行。在上线 ERP 产品的时候应把企业的长远发展也考虑进来，可以优先上线其中的一个模块或几个模块，随着企业发展需要再上线其他模块或修改已有模块，这样也便于后续的设计和实施。

其次是软件实施的人力资源风险。人力资源是 ERP 实施中最关键的资源，保证合适的人，以足够的精力参与到项目中来，是项目成功实施的基本保证。企业上 ERP 是“一把手工程”，但集团高层在调整的过程中，更多地是关注企业的生存，企业经营的合理化和利润最大化，显然没有认真考虑结构调整对 ERP 项目的影响，“一把手”的有效推动和支持作用没有贯彻到 ERP 项目的始终。

在美国，由于各种原因导致 ERP 软件实施失败引起的法律诉讼不断。

2011 年 2 月，美国加州马林郡(Marin County)政府向联邦法院状告 SAP 与德

勤咨询公司，声称这两家公司利用 ERP 项目故障敲诈他们 2000 多万美元。在诉讼中，SAP 与德勤咨询公司被控告违反了联邦诈骗影响及腐败构成法(RICO)。根据该法案条文的规定，该郡主张的 3500 万美元损失将得到 3 倍赔偿。马林郡政府还表示，SAP 在营销过程中利用引诱的手段使其成为软件早期试用者计划中的一员，而由软件自身的不成熟所带来的风险最终导致了项目整体的失败。

2011 年 5 月，位于美国新泽西州的蒙特克莱尔州立大学与甲骨文公司对簿公堂，宣称这家老牌企业所提供的 PeopleSoft 项目彻底失败了，根本无法取代学校现有的陈旧遗留系统。校方指控，由于甲骨文的不当处理方式，该项目的实际开支可能高达 2000 万美元。不过甲骨文迅速进行了回击，声称整个问题完全是校方的负责。甲骨文在法庭陈词中辩称：“在项目实施过程中出现问题时，很明显蒙特克莱尔州立大学的校领导们对于完成项目所必需的技术与步骤缺乏充分了解。校方没有与我方通过讨论及交流来通力合作进而解决问题，反而因为害怕因工期延误而受到指责而盲目制定议程，最终导致普通的管理差异升级为严重的法律纠纷。”蒙特克莱尔州立大学校方最近刚刚提交了一份经过修订的申诉，在其中添加了更多详尽的细节陈述，包括甲骨文在营销过程中“伪造”软件演示效果等问题，并就此提出索赔。

2012 年 9 月至 2013 年 1 月，Panorama consulting solutions 历时 4 个月进行了 ERP 实施成功率的调查，其中参与者的企业营业额 71%是 3 亿美金以下，21%达到了 10 亿美金或更高。调查显示，超过 50%的项目超过了预算；超过 60%的项目超出了计划的时间；60%的企业从 ERP 项目中获得的收益低于预期的一半。调查的数据也显示了一个关于 ERP 成功与否的矛盾结果，尽管多数的 ERP 实施完成的晚、超过预算且没有达到计划的结果，但是只有 10%的人愿意承认他们的 ERP 项目失败了。这和我们国内的现状相似，ERP 可能未实施成功或者未达到预期收益，但很多企业由于种种原因，即使失败了也没人喊冤。

经过多年的实践和发展，ERP 服务商拥有更加成熟的规划实施方法论，产品走向标准化、精细化和行业化，企业对于 ERP 的认知度和自身的信息化素质也在不断提高，但这并不意味着企业的 ERP 应用就一定能成功。伴随着业务的复杂性和市场的快速变化、各种系统间的整合，企业的信息系统愈加复杂，大数据、社交媒体、云计算、移动终端和商务智能等新技术的发展，企业的 IT 决策人员和

ERP 建设面临着众多挑战，企业必须通过有效的管控措施才能降低 ERP 项目实施失败的风险。

概 念 释 义

信息系统与信息化术语

（锐思咨询技术法规部）

术语	释义
EIP 系统	EIP 系统是企业的电子门户系统，建立在协同商务的概念之上。它支持一个企业的员工、客户以及合作伙伴进行交流的平台，还支持与其他管理系统的连接。
IT 规划	是指在理解企业发展战略和评估企业 IT 现状的基础上，结合所属行业信息化方面的实践和对最新信息技术发展的认识，提出企业信息化建设的远景、目标和战略，以及具体信息系统的架构设计、选型和实施策略，全面系统地指导企业信息化建设，满足企业可持续发展的需要。
企业信息化	企业信息化实质上是将企业的生产过程、物料移动、事务处理、现金流动、客户交互等业务过程数字化，通过各种信息系统网络加工生成新的信息资源，提供给各层次的人们洞悉、观察各类动态业务中的一切信息，以做出有利于生产要素组合优化的决策，使企业资源合理配置，以使企业能适应瞬息万变的市场经济竞争环境，求得最大的经济效益。
企业信息管理	所谓企业信息管理是指为企业的经营、战略、管理、生产等服务而进行的有关信息的收集、加工、处理、传递、储存、交换、检索、利用、反馈等活动的总称。 企业以先进的信息技术为手段，对信息进行采集、整理、加工、传播、存贮和利用的过程，对企业的信息活动过程进行战略规划，对信息活动中的要素进行计划、组织、领导和控制的决策过程，力求资源有效配置、共享管理、协调运作，以最少的消耗创造最大的效益。
企业信息化建设	企业信息化建设是指企业利用计算机技术、网络技术等一系列现代化技术，通过对信息资源的深度开发和广泛利用，不断提高生产、经营、管理、决策的效率和水平，从而提高企业经济效益和企业竞争力的过程。从内容上看，企业信息化主要包括企业产品设计的信息化、企业生产过程的信息化、企业产品销售的信息化、经营管理信息化、决策信息化以

术语	释义
	及信息化人才队伍的培养等多个方面。
企业信息能力	企业信息能力是企业家借助企业内部的组织机构对信息分散获取、处理和利用的能力，是其个人信息能力的延伸。
实时企业	实时企业是四个字的关联词，并不是指一个企业，而是指运营企业的一个理念。这个理念也可以说是一种企业文化，管理哲学。这个理念就是企业负责人和工作人员随时可以了解企业的竞争环境，企业的物流、信息流、资金流的进出情况，并根据以前的经验，做出正确而快速的反映。实时企业理念的核心就是要企业建立一套“企业神经系统”。
数据分析	数据分析是指通过建立审计分析模型对数据进行核对、检查、复算、判断等操作，将被审计单位数据的现实状态与理想状态进行比较，从而发现审计线索，搜集审计证据的过程。
数据管理	数据管理是对不同类型的数据进行收集、整理、组织、存储、加工、传输、检索的各个过程，它是计算机的一个重要的应用领域。其目的之一是从大量原始的数据中抽取、推导出对人们有价值的信息，然后利用信息作为行动和决策的依据;另一目的是为了借助计算机科学地保存和管理复杂的、大量的数据,以便人们能够方便而充分地利用这些信息资源。数据管理是数据处理的核心，是指对数据的组织、分类、编码、存储、检索、维护等环节的操作。
数据质量管理	数据质量管理是指为了满足信息利用的需要,对信息系统的各个信息采集点进行规范，包括建立模式化的操作规程、原始信息的校验、错误信息的反馈、矫正等一系列的过程。
数据采集	数据采集是指将被测对象的各种参量通过各种传感器做适当转换后,再经过信号调理、采样、量化、编码、传输等步骤传递到控制器的过程。
信息管理	所谓信息管理是指在整个管理过程中，人们收集、加工和输入、输出的信息的总称。信息管理的过程包括信息收集、信息传输、信息加工和信息储存。
信息生命周期管理	信息生命周期管理是，信息在储存媒介网络之内流动的过程，而这种过程需要确保企业获取需要的商业信息,并向客户提供一个良好的服务水

术语	释义
	平，同时把单位成本降到最低。ILM 还要满足日益增长的对于成熟和自动化存储管理的需求,这可以在保持企业对于商业环境变化做出快速反应的能力的同时，提高个人的工作效率。这一种定义强调的是过程的概念。
信息化管理	信息化管理是以信息化带动工业化，实现企业管理现代化的过程，它是将现代信息技术与先进的管理理念相融合，转变企业生产方式、经营方式、业务流程、传统管理方式和组织方式，重新整合企业内外部资源，提高企业效率和效益、增强企业竞争力的过程。
信息资源	信息资源是企业生产及管理过程中所涉及到的一切文件、资料、图表和数据等信息的总称。它涉及到企业生产和经营活动过程中所产生、获取、处理、存储、传输和使用的一切信息资源，贯穿于企业管理的全过程。信息资源与企业的人力、财力、物力和自然资源一样同为企业的重要资源，且为企业发展的战略资源。同时，它又不同于其它资源（如材料、能源资源），是可再生的、无限的、可共享的，是人类活动的最高级财富。
信息资源规划	信息资源规划是指对企业生产经营所需要的信息，从采集、处理、传输到使用的全面规划。在企业的生产经营活动中，无时无刻不充满着信息的产生、流动和使用。要使每个部门内部，部门之间，部门与外部单位的频繁、复杂的信息流畅通，充分发挥信息资源的作用，不进行统一的、全面的规划是不可能的。
信息成本	在多数情况下，信息并不形成企业产品实体，这与人力不构成产品实体的道理是一样的。信息产品的品种也纷繁多样。从本质上说，任何可以被数字化(编码成一段字节)的事物都是信息。信息对不同的消费者有不同的价值，不管信息的具体来源是什么，人们都愿意为获得信息付出代价。
信息安全管理体系	信息安全管理体系是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的体系。它是直接管理活动的结果，表示成方针、原则、目标、方法、过程、核查表（Checklists）等要素的集

术语	释义
	合。
信息孤岛	所谓的“信息孤岛”，是指相互之间在功能上不关联互助、信息不共享互换以及信息与业务流程和应用相互脱节的计算机应用系统。
信息治理	即领导、指导、控制、提供保障的行为或过程，通过这些行为或过程，信息被当作贯穿于整个企业的企业资源得以有效管理，其中包括解决信息冲突问题方面的管理。
信息泄密	信息泄密指重要信息在有意和无意中被泄露和丢失。如信息在传递、存储、使用过程中被窃取等。
信息侵权	信息侵权是指对信息产权的侵犯。传统的信息产权主要是指知识产权，包括版权、专利权和商标权。现代信息技术环境中的信息侵权除了侵犯著作权、专利权和商标权外，还会出现计算机软件侵权，数据库产品侵权、域名侵权、网上信息侵权等。
信息系统生命周期	信息系统生命周期是指信息系统在使用过程中随着其生存环境的变化，要不断维护、修改，具有产生、发展、成熟、消亡(更新)的过程周期循环。
信息系统结构	信息系统结构是信息系统内部各个组成部分所构成的框架结构。
信息系统维护	信息系统维护是指为适应系统的环境和其他因素的各种变化、保证系统正常工作而对系统所进行的修改，包括系统功能的改进和解决系统在运行期间发生的问题。
战略信息管理	从理论来源的角度考察，战略信息管理可以视作战略管理与信息管理的交集，是一种跨领域的管理活动； 从战略规划的角度考察，战略信息管理可以视之为信息战略的展开过程，是企业信息功能战略的制订、实施、监控、调整及其与企业业务战略的整合过程； 从领域分析的角度考察，战略信息管理可以视之为一个跨越所有企业活动领域的相对独立的功能领域，是围绕信息、信息技术、信息人员、信息设备及其它相关资源实施规划、预算、组织、指挥、控制、协调和培训等活动的多功能领域。

术语	释义
云计算	云计算是基于互联网的相关服务的增加、使用和交付模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源。云是网络、互联网的一种比喻说法。过去在图中往往用云来表示电信网，后来也用来表示互联网和底层基础设施的抽象。狭义云计算指 IT 基础设施的交付和使用模式，指通过网络以按需、易扩展的方式获得所需资源；广义云计算指服务的交付和使用模式，指通过网络以按需、易扩展的方式获得所需服务。这种服务可以是 IT 和软件、互联网相关，也可是其他服务。它意味着计算能力也可作为一种商品通过互联网进行流通。
主数据	主数据是指在整个企业范围内各个系统(操作/事务型应用系统以及分析型系统)间要共享的数据，通常需要在整个企业范围内保持一致性(consistent)、完整性(complete)、可控性(controlled)。

锐思咨询

Less Risk, More Value

联系我们：

上海市九江路 69 号 5 楼（古象大厦）

400-659-8166

mail@lx-rs.com

www.lx-rs.com

@锐思咨询-风险管理与内控