审计新视野译丛

WILEY
Publishers Since 1807

ERP系统整合审计

[加] 尤苏费利·F·穆沙基(Yusufali F. Musaji) 著
[匈] 阿什·胡克(Ash Huq) 著
陈明坤 / 译

Integrated Auditing of ERP Systems

经济科学出版社
Economic Science Press

审计新视野译丛

ERP 系统整合审计

[加] 尤苏费利·F·穆沙基 (Yusufali F. Musaji)
[匈] 阿什·胡克 (Ash Huq) 著

陈明坤 译

经济科学出版社

责任编辑:王长廷　周国强　杨爱君
责任校对:杨　海
版式设计:代小卫
技术编辑:邱　天

ERP 系统整合审计

[加]　尤苏费利·F·穆沙基(Yusufali F. Musaji)
[匈]　阿什·胡克(Ash Huq)　著
陈明坤　译

经济科学出版社出版、发行　新华书店经销
社址:北京市海淀区阜成路甲 28 号　邮编:100036
总编室电话:88191217　发行部电话:88191540
网址:www. esp. com. cn
电子邮件:esp@ esp. com. cn
北京密兴印刷厂印装
690×990　16 开　14.125 印张　230000 字
2007 年 1 月第一版　2007 年 1 月第一次印刷
ISBN 978-7-5058-5961-6/F·5222　定价:38.00 元

图书在版编目(CIP)数据

ERP 系统整合审计/(加)穆沙基,(匈)胡克著;陈明坤译.
—北京:经济科学出版社,2007.1
(审计新视野译丛)
书名原文:Integrated Auditing of ERP Systems
ISBN 978-7-5058-5961-6

Ⅰ.E... Ⅱ.①穆...②胡...③陈... Ⅲ.审计—计算机管理系统,ERP Ⅳ.F239.1

中国版本图书馆 CIP 数据核字(2006)第 144365 号

图字:01-2006-5355

Integrated Auditing of ERP Systems
Yusufali F. Musaji

前言

本书重点讲述ERP生命周期中各种阶段出现的主要概念，以及ERP系统中需要审计人员重点掌握的组成部分。本书将详细介绍ERP系统自带的控制程序，并将推荐一些对审计有重大意义的控制程序。本书还为信息安全审计师以及IT部门提供了一些有用的建议，并为企业进行整合审计提供了一些控制设计方法。

虽然本书的写作目的是为了审计部门进行审计工作，但是它还有其他更广泛的用途。在ERP生命周期的各个阶段中，管理者会对各部门控制程序的有效性进行评估，这本书便会提供相应的帮助。审计人员可以利用本书所提供的知识与技巧，设计审计程序，评估和测试企业对ERP系统的运行控制情况。

最后，企业可以利用本书为普通审计人员、IT审计专家、内部审计师以及其他人员开发培训课程。各种水平的审计人员都有必要接受企业培训并具备一定的IT审计实际经验，这两点也是整合审计的基础。目前，越来越多的企业使用计算机，因而计算机系统也越来越小，运行速度也越来越快，价格也越来越低。本书的重要性也会不断提高。

作者简介

尤苏费利·F·穆沙基(Yusufali F. Musaji)，加拿大注册会计师(CGA)、信息系统注册审计师(CISA)、信息系统安全认证专家(CISSP)，爱丽丝NY咨询公司的创始人、董事长及总经理，该公司是一个IT和财务咨询公司，尤以IT图书出版而享誉业界。穆沙基先生的从业经验涉及任何优秀企业所必需的财务、经营及IT知识。

阿什·胡克(Ash Huq)，德勤会计师事务所(Deloitte & Touche)风险管理部高级经理，在信息系统评估、信息系统实施、会计、风险管理以及SAP R/3系统的安全和控制领域有长达18年的从业经验，是本书的合著者。

目　录

第 1 章

ERP 系统实施概述

今日事今日毕

——马克·吐温

1.1 引 言

实施企业资源计划系统(Enterprise Resource Planning, ERP)既是一门 1
艺术也是一门科学,它由制定计划、系统实施、系统维护三个部分组成。本章所讲的结构化方法实现了实施 ERP 系统的自动化,并通过列明、图解和论证所有步骤提供了解决问题的办法。该方法把 ERP 的实施和维护看作一门工程学学科而非软件开发人员的突发奇想,从而有利于 ERP 实施及维护过程的标准化和系统化。在 ERP 系统的实施过程中,掌握结构化方法非常关键。

结构化方法的基本步骤包括:

- 项目定义和需求分析。明确权责范围,明确用户需求和系统限制,提出最优解决方案所需的系统功能要求和逻辑模型。
- 外部设计。对一个选定的解决方案进行详细设计,包括所有跟程序相关的图表、子路线和数据流。
- 内部设计。构建,测试,安装和调试软件。 2
- 系统实施前。评估和验收系统。
- 实施阶段。实施系统。
- 系统实施后阶段。评估系统控制情况并解决系统运行中出现的问题。

本书讲述了 ERP 系统，系统生命周期及其主要组成部分，以帮助读者了解任何一种主流的 ERP 产品。本书讨论了 ERP 生命周期的各个阶段，包括每个主要参与者的角色，关键事务及交付成果等。本书对审计角色给予了特别关注，它是以后各章节的焦点。如果其他参与者未能充分发挥他们的作用，则很可能需要对审计工作做出相应的调整。

某组织购买 ERP 系统的动机是该系统具备某些功能并为该组织带来效益。但购买之前，企业必须明晰这些功能以及其所带来的收益，确保此系统能够达成企业所希望的效果。这个过程称为可行性分析。进行可行性分析的目的是：

- 分析企业目标、需求及澄清系统概念。
- 对可以实现目标的不同方案进行评估。
- 提议执行某一方案。

可行性分析通常包括：

- 当前工作惯例。经过深入调查，揭露出企业存在的重复劳动，或者那些很早之前制定的、现在仍在执行但已不再需要的程序。
- 信息渠道。对此进行考察的原因是可行性分析主要与每个内部系统输入输出信息相关。这种分析不存在部门界限和偏见。当企业真实的信息传播模式被披露后，企业通常会对资源进行重组，从而获取用以决策的所有相关数据信息。
- 备选方案。企业应该全面考虑处理或提供信息的不同方法。
- 成本因素。这些因素必须清楚地识别出来，明确实施该系统节省了多少成本或增加了多少收益。企业必须考察现有成本，以便与系统实施后成本相比较。由于显示出的结果与信息结构相关而与部门组织无关，所以新方案可能提出一些隐藏在现有系统中的仍可改进的措施。
- 提供支持性的服务。在系统安装期间，应当对有关人员进行培训并有专人帮助员工使用这些系统和程序。
- 兼容性程度。如果工作量扩大的话，是否能提升配置而不需要大规模地重新编程。

下面将讨论传统审计（例如财务、经营和 IT 审计）与计算机环境下的整合审计之间的异同。同时，还将设定 ERP/IT 控制目标，并将其作为 ERP 系

统审计的标准。

整合审计

“整合审计”一词最早起源于IT界术语“集成数据”,“集成数据”之后又出现了“集成系统过程”和“系统集成过程”,ERP系统就产生于系统集成过程。ERP系统定义如下:通过引入集成界面、集成数据集和集成代码集来实现公司业务处理过程自动化的一种信息系统。因此,从纯商业的角度讲,将各种信息完全整合起来以实现与技术发展同步,对审计人员的工作非常有利。

在ERP系统出现之前,企业将很多重要的商业信息储存在许多不同的部门,各部门用于管理这些信息的系统和技术也不同。有时某种信息在企业内部多次复制,但是其中有些部门并不需要这些信息。还有一些书面信息使得其在部门间的传阅比较困难。例如,客户可能打电话到销售部门查询一个重要订单的进展情况,为回答这个问题,销售部门因无共享数据库可查,而不得不打电话到公司的生产或货运部门查询订单进展情况。

在一个典型的制造企业里,产品相关数据被存放在下列多个不同的部门:

- 存货余额信息存储在存货控制部门。
- 产品成本或标准成本信息存储在成本管理部门。
- 按生产量发放奖金的奖励制度存储在员工激励部门。
- 生产账户所需的存货价值信息存储在财务/会计部门。
- 货运和接货部门保存着发货量和已收原材料的数量信息。
- 退货部门保存着已退存货的信息。
- 还有其他部门保存的其他信息。

ERP系统最初是为了满足制造企业的信息需求。随着时间的推移,它已经被应用到其他行业,包括健康医疗、金融服务、航空业以及消费品行业。ERP系统在转移到客户机/服务器系统之前,最初是在大型机器上运行的。随着ERP系统的不断发展,它现在已经转移到了网页上并且包含了许多应用程序。

ERP系统的一个重要商业目标是使企业的各个部门均能知道本企业正在做什么,并且某部门可以从中获取所需数据以便更新记录。

ERP 系统的最主要特征是把跟同一主题相关的分散的记录合并为一项记录存放在计算机里。新的产品记录包括所有相关数据，而在以前，这些数据被分散在6个甚至更多不同的记录中。不难想像这些分散在不同部门的信息给企业造成很大的困难(即安全性、保密性、准确性、完整性和可靠性)。

5 集成系统的第二个特征是只需向计算机输入一次数据便可更新所有相关信息，不再像以前那样需要多次记录、转抄数据才能完成。况且，应用集成系统之前，企业还要费尽周折及时对各部门进行协调，做好信息收集的时间安排等等，一次性输入计算机的做法也称为单点进入，便解决了上述问题。

通过各种合适的计算机程序(比如软件、应用程序、函数或计算机联合等等)，不同部门所需的所有信息都能够随时获得。这是计算机通过处理存放在产品主文件或者集成数据库中的集成记录实现的。集成系统把传统上独立的系统联合起来，消除了部门之间的界限。

ERP 系统的共性能带来巨大的效益，包括减少失误，加快信息处理速度与效率，更多的部门可以共享企业信息。由于企业员工和管理层能够更容易地获取企业信息，因而更容易了解企业的发展动态，也就能以此做出更佳的决策。例如，在 ERP 系统中，采购部门的采购人员可以看到客户订单的增加或减少，便能够快速调整材料采购量。结果呢？他要么保证了原材料的及时供应，要么节省了存货支出。

整合审计应当确保控制是不可复制的。一个部门的有效控制不会导致另一个部门的控制失效。控制的总目标是确保在最佳时机进行产品营销。审计人员通过互相交流，应当能够提高控制的功效。

在平台上实施 ERP 系统有时并不容易，因为它需要对很多问题进行重新设计，包括安全性、质量保证以及组织员工进行 ERP 系统应用的培训。

6 除了要实现 ERP 系统的操作效率最大化外，IT 经理、系统安全人员以及系统开发人员在安全和控制问题上会遇到很多困难。

ERP 环境下的审计目标

在 ERP 环境下，对控制进行审计的基本目标并没有改变。企业在评估其对 ERP 系统的控制时，必须确定操作性内部控制程序是否与信息技术(IT)控制相适应。因此企业必须对实现审计目标所需的具体控制程序进行测试。

企业应向审计人员提供控制程序和样本测试合格的相关资料。资料应尽可能地详细,由审计人员选读,考察系统是否与当前审计的环境相适应。

除了主要的审计责任,审计人员应当指出如何改进企业的控制程序。审计人员应当把系统存在的重大脆弱点传达给有关的IT部门。审计人员还应当对那些需要特别检查的控制弱点保持应有的谨慎,并且应在评估现有系统的同时对正处于开发过程的系统进行评估。

ERP系统架构

ERP系统应当及时输出准确、完整并经过授权的信息。在计算机环境下,这些信息由ERP系统中的控制程序与ERP系统运行环境中的控制程序(包括操作系统)联合产生。控制可分为一般控制和应用控制。一般控制又分为管理控制和环境控制。管理控制用以处理组织、政策、程序、计划等问题。环境控制指由计算中心/计算机操作群执行的运营控制以及计算机自带的操作系统控制。

ERP系统与ERP系统处理和存储的数据的财务和(或)运营敏感性同样关键。ERP系统的安全性可以用一个金字塔来表示(见图1.1)。金字塔的最底部是硬件的物理安全,这些硬件包括机器、数据库以及脱机存储媒介 7
(如录音带或磁带)。第二层涉及计算机操作系统。第三层主要指安全软件。在大型计算机环境下,企业要安装诸如ACF2或TOP Secret的安全软件。若公司安装的是诸如UNIX或AS/400的操作环境,可以把安全软件安装在操作系统中。安装安全软件的目的是为了保护内核、优先权状态以及为操作系统和硬盘腾出空间。另外,它也是为了防止ERP系统直接访问操作系统和硬件,这也是保证操作系统安全的基础。金字塔的第一层至第三层对保证计算机环境的安全起了很大作用,《审计与安全、AS/400、NT、UNIX、Network和DRP》对此进行了详细探讨。在环境安全的前提下,如果企业生产数据和过程发生变化,ERP系统将保证财务与运营情况的一致性。反之便会出现不一致的现象。

在此,ERP系统与ERP系统运行的计算机环境是区别对待的。事实 8
上,它们并非相互排斥和独立,两者相互影响。本书重点关注ERP系统,假设企业拥有一套大型网络系统,用以存储、处理或传输敏感数据和信息。

企业资源计划是由多模块应用软件支持的众多行为的集合。这些多模块应用软件帮助制造商或其他形式的企业管理其商务行为的重要部分,包

括产品计划、零部件采购、维持存货、与供应商交流、提供客户服务以及追踪订单。ERP 系统还包括企业用于财务和人力资源管理方面的应用程序模块。ERP 系统通常要使用某一相关的数据库系统或与之集成。企业还可以利用 ERP 系统进行业务流程分析、就业再培训分析和新工艺分析。

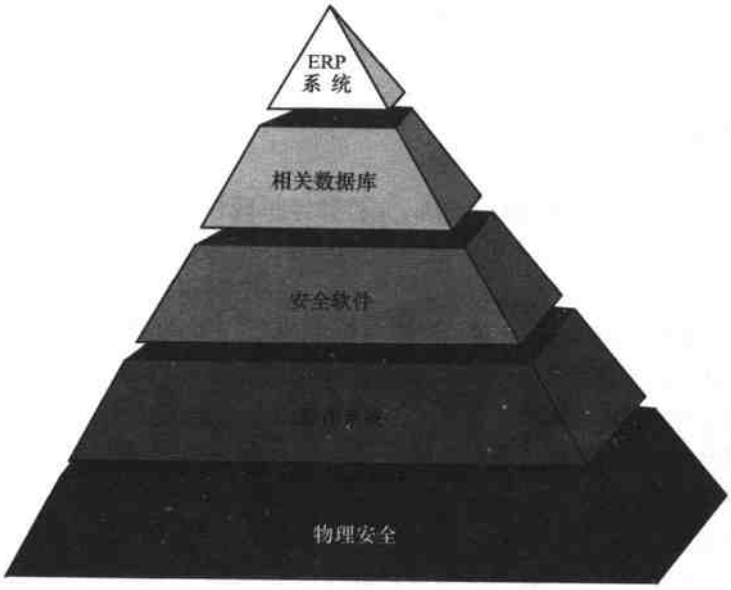

图 1.1

ERP 系统以前的系统利用平面文件和传统的 IBM 索引顺序存取方法(ISAM)和虚拟顺序存取方法(VSAM)来存储数据和信息,而 ERP 系统用的是关系数据库。一个关系数据库是一些数据项的集合。它们由规范描述的列表集合组成,从这些列表中可以获取数据或者通过各种方式对数据重新进行组织,而不必重新组织数据库列表。

关系数据库的标准用户/应用程序界面是结构化查询语言(SQL)。结构化查询语言既可以用于查询关系数据库中的信息,又可以为某些报告采集数据。

关系数据库除了具备创建和获取信息相对容易的优点外,它还有一个很重要的优点即易于扩展。在原始数据库中,无须修改任何应用程序,便可以加入一种新的数据类型。

关系数据库是一组列表的集合,这些列表用来存放预先定义好数据类

型的数据。每张表(有时也称为一个关系)包括一种或多种列数据类型,每行包括一个惟一的数据记录,该数据类型为所在列的数据类型。例如,通常情况下企业订单输入数据库都包括一张描述顾客信息的表,第一列是客户姓名,第二列是客户地址,依次类推,第三列为客户电话等等;另一个描述订单的列表,记载了某订单的产品名称、客户名称、订单日期、销售价格等等。用户可以利用由这些列表组成的数据库找到自己所需的信息。例如,其分公司的经理可能需要一份在某一特定日期后购买了本公司产品的所有客户名单。同一公司的财务经理可以从同一数据库中获得应收账款的信息。

1.2 ERP系统的特征

当大多数人谈及"核心"ERP应用程序或"模块"时,他们指该系统的后台管理人力资源、会计与财务、生产和项目管理功能。然而,甲骨文公司(Oracle)、人民软件公司(PeopleSoft)和SAP公司等大企业提供的主流ERP产品不仅具备上述这些功能,还包括销售自动化、商业智能、客户关系管理以及供应链管理等功能。

尽管我们检查、评价和测试控制框架的目标是相同的,但是ERP系统与非ERP系统之间存在重大差别。这些差别有:

- 在ERP系统中,某些控制程序不会留下反映其控制效果的证明文件,而对另外一些程序来说,证明文件不能直接获得,它可能包括在编程逻辑或操作指令中。因此,在ERP系统中,符合性测试的结构可能不同,因而对用户程序的考察可能变得尤为重要。
- 在ERP系统中,信息经常是以电子表格的形式保存,而离开计算机这些信息便不可读。
- ERP系统通常是基于之前输入的数据自动产生财务和交易信息,而无须手工操作。
- 由于人工参与计算机处理的情况减少,一些在非ERP系统下可以察觉的错误,此时却不易被发现。这些未被发现的错误有可能被扩散到大量的信息处理中,这种情况对企业信息管理非常不利。
- 借助于正确的控制,ERP系统比非ERP系统更可靠。这是因为ERP系统的所有数据由相同处理程序和控制程序所控制,非ERP

系统可能因随机的人工失误而产生错误。然而，尽管计算机处理过程未变，但错误仍有可能发生，例如，计算机程序出错。

- 在 ERP 系统付诸实施之后，就很难对它进行变动。因此，我们应当弄清楚企业是要引进重要的新系统还是只在现有的系统上做些重要改动。在新系统实施之前对新系统或者重大修改进行审核是企业的正确选择，这样，可以对控制程序的适用性进行初步评估以确定合适的审计轨迹以及是否需要对审计方法做任何改变。

ERP 系统的类型很多，从最简单的批控制类型到复杂的集成应用程序类型。集成应用程序类型的 ERP 系统可以同时实现多个功能。

批控制系统

在计算机中，批处理是由计算机实现非交互式运行的一种程序。例如，一个打印请求或者是一次网页日志的分析。在大型的商业计算机或服务器中，批处理工作通常是由系统用户发起的。一些批处理工作被设定在特定时间内自动运行完成。

在有些 ERP 系统中，批处理工作在后台运行，交互程序在前台运行。一般来说，交互程序优先于批处理程序得到执行，批处理程序在交互程序等待用户请求时的间隔期间内运行。

“批处理”一词源于计算机输入的最常见形式——穿孔卡片。那时，计算机操作员把一批批排好序的卡片插入计算机（结果有望在第二天早晨输出）。

在一个典型的批处理系统中，各用户定期向工厂部门提交一批批的交易数据由工厂部门进行转录和处理。批处理总数通常由人工计算得出，然后建立相应数目的批控制程序，这些控制经过后续处理阶段的协调，生成文件更新报告或最终打印结果。

计算机最初产生时，批处理系统占主导地位。现在，许多组织机构都开始使用下述更高级的系统。

在线系统

在计算机中，交互活动是发生在人（或者是另外一种生物）与计算机程

序之间的一种对话(那些不需要用户直接参与就可以运行的程序不是交互的,它们通常被称为批处理程序或后台程序)。游戏软件经常促成大量交互活动,订单输入程序以及其他许多商业应用程序也是交互的,只是交互形式有所限制,用户交互行为较少。这些程序提供的可供用户交互的选项更少。

万维网不仅仅提供与浏览器(网页应用程序)的交互,而且也提供与浏览器上的其他网页的交互。这种被称作超链接的隐性邀请连到其他网页上,并在网站上提供最常见的互动行为(这种网络之间的互动行为可以被看作一个巨大的相互关联的应用程序)。

除了超链接之外,网页(以及计算机系统中的许多非网页应用程序)还提供其他一些交互活动的可能性。任何形式的用户输入,包括键入指令或者点击鼠标,都是一种输入形式,显示的图像和文本、打印出的资料、动画录像以及声音等都是交互活动的输出形式。

最早与计算机互动的形式是间接的,先把指令提交到穿孔卡片中,然后由计算机读出并执行相应的指令。后来,计算机系统被设计成普通人(而不仅仅是程序员)就能够直接与其进行交互活动,告诉它们要运行什么程序。人们可以与文字处理软件(又叫编辑器)、绘画程序以及其他交互程序进行交互。第一个人机交互界面是输入一文本序列,被称为"指令"(如"DOS指令"),然后系统就会出现一行简短的反应。

在20世纪70年代后期,第一个图形用户界面(Graphical-user interfaces, GUIs)在Xerox PARC实验室诞生,后来它们被引入到了Apple Macintosh的个人电脑中,然后又被引入到微软的Windows操作系统里,如今,几乎在所有的个人电脑里都有图形用户界面。

图形用户界面(通常被读作Goo-ee)是指一种图形用户与计算机之间 12
的交互界面(而不是纯文本用户交互界面)。当你读到这里时,也许你正在盯着网页浏览器的图形用户界面看呢。这个术语之所以存在是因为第一个用户交互界面不是图形的,而是由文本和键盘来实现,通常由一些需要用户记忆的指令组成,计算机的回应却异常简单。在图形用户界面出现之前,DOS操作系统(你现在仍然可以从Windows操作系统中进入此操作系统)的指令界面是一个典型的用户—计算机界面交互实例。处于指令行界面和图形用户界面之间的是非图形、基于菜单的界面,在这种界面中,你可以通过点击鼠标而不是键盘来键入指令与计算机进行交互。

当前主流的操作系统都支持图形用户界面。应用程序在利用操作系统