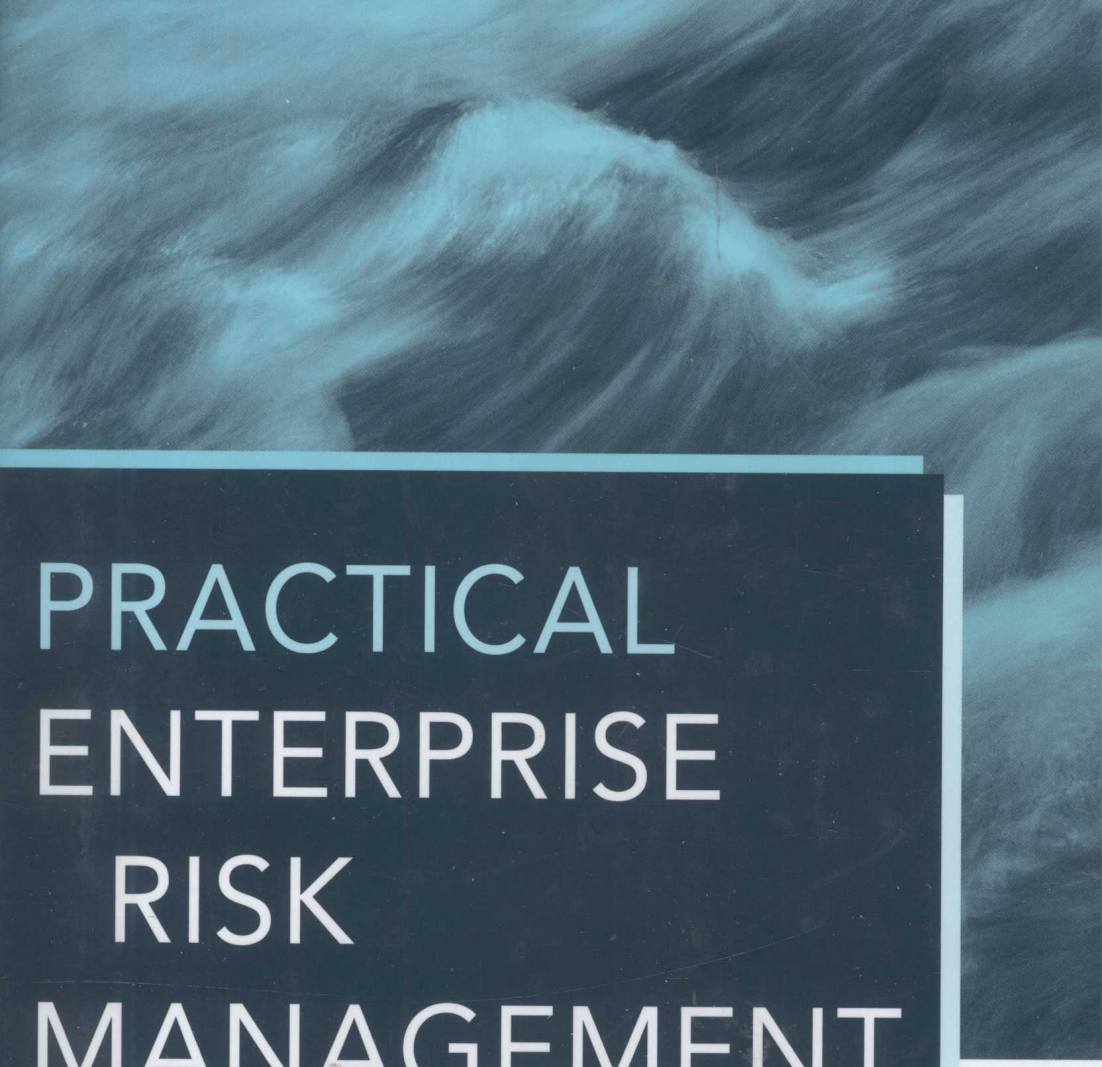

PRACTICAL ENTERPRISE RISK MANAGEMENT

A Business Process Approach

GREGORY H. DUCKERT

Practical Enterprise Risk Management

A Business Process Approach

GREGORY H. DUCKERT

WILEY
John Wiley & Sons, Inc.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:
Duckert, Gregory H., 1949-
Practical enterprise risk management : a business process approach / Gregory H. Duckert.
p. cm.
Includes index.
ISBN 978-0-470-55985-7 (cloth); 978-0-470-89251-0 (ebk); 978-0-470-89252-7 (ebk); 978-0-470-89253-4 (ebk)
1. Risk management. I. Title.
HD61.D85 2010
658.15'5—dc22
2010016278

Printed in the United States of America
10 9 8 7 6 5 4 3 2 1

Preface

THIS BOOK IS INTENDED to be a handbook of *how to* establish a highly effective enterprise risk management (ERM) environment that is actually a business tool that yields real business value. This book is a definitive guide for members of the Boards of Directors, the C Suite, Chief Risk Officers (CROs), and those charged with ERM, as well as all levels of management. In addition, this book is a must have for any shareholder who owns stock in any publicly listed corporation and should be read cover to cover to understand why she should be concerned. This is a how-to, hands-on guide, not a generic framework scenario.

With the advent of corporate business catastrophes such as Enron, WorldCom, Lehman Bros., General Motors, and so on it behooves corporate executives to get better connected with their businesses. In addition, the government has now initiated a number of regulatory activities, including Sarbanes-Oxley, which further complicate the lives of the auditors and the corporate executives. The only way to be truly in compliance with Sarbanes-Oxley is to be well aware of what is going on in your corporation, virtually daily. To accomplish this, it is necessary for corporations to establish a highly effective information-centric risk assessment methodology. Without such a methodology intricately woven into the fabric of the organization, it is virtually impossible to guarantee any type of compliance in a realistic fashion. Enterprise-wide risk assessment is much more than simply a catchy phrase or the latest in a string of failed corporate initiatives. If properly constructed, it can be a highly effective governance and oversight tool, which becomes almost irreplaceable in the arsenal of tools necessary for progressive organizations today.

Of interest is that the Chairman Emeritus of the Committee of Sponsoring Organizations (COSO), Larry Rittenberg, PhD., CPA, CIA attended the session I presented for the Madison, Wisconsin, chapter of the IIA on Enterprise-Wide Risk Assessment in 2001. The entire discussion was focused on the concept of

using data to evaluate risk throughout an organization. In the presentation, real-time triggers, key process indicators, key risk indicators, Metric Oversight Monitoring Systems (MOMS), and numerous other concepts were discussed for consideration by the participants. I have used these and other similar tools during 30 years of data-centric risk assessment. These tools and methodology will be discussed in this book.

Dave Coderre, a very talented ACL practitioner and author, published the GTAG (Global Technology Audit Guide) on Continuous Auditing in which he presented a very convincing argument for the necessity of continuous audit tools, continuous monitoring, and continuous risk assessment. All of these advanced methods, of course, revolve around the utilization of data. I had the great pleasure of having Dave Coderre as a participant in one of my risk assessment sessions discussing the use of data-driven risk assessment a number of years ago. It is excellent to see that the subject matter is finally getting some serious discussion at these levels.

This book is meant to be a reference point for all organizations that are engaged in or will be engaged in the exercise of establishing an enterprise-wide risk assessment and management oversight system for their organization. It presents an alternative approach to the models that are most commonly seen. In keeping with the underlying thought process of this book, it is straightforward and to the point. This book is not an exercise in overcomplicating a straightforward issue. There are many people who believe that complexity adds value to a process or a methodology. I am not one of them. The whole premise of the book is that complexity in most cases adds nothing to a business process but complexity.

A risk model is no exception. The reality of the matter is that when a risk model becomes overly complex it also becomes unusable. Therefore, as we proceed from this point forward, everything will be clearly expressed and understandable. There will be no complex theories to entangle endlessly what is actually a very commonsense subject matter. Under no circumstances will there be any abstract theories or unattainable methodologies employed.

The approach to risk assessment undertaken in this book is based upon fact, common sense, and practical methodologies for implementation. The model also eliminates subjectivity and guesswork as much as possible. The model presented parallels the normal operation of the business, be able to be effectively utilized at all levels of the business, and can be truly used to create an all-encompassing risk model.

In Chapter 1 I discuss the subject of corporate governance and what is wrong with it in its current format. In addition, I call attention to one of the

major shortcomings of most corporations and one of its biggest risk areas, which is systems implementation.

In Chapter 2 I address what I believe to be a significant misunderstanding relative to the subject of risk and risk management. Essentially every model that is out there to perform any type of enterprise risk management is based upon the premise of subjective scoring to arrive at a conclusion. Subjective models are always time and space dependent, and therefore inconsistent. In other words, the same exact situation will always be viewed differently by the exact same person on a different day in a different environment or on a different hour in the same environment.

In addition, when dealing with the subject of risk, you must be prepared to estimate probability and impact or exposure; these models attempt to deal with the subject matter via scoring and unexplainable calculations. Anybody that is the least bit familiar with risk or risk management knows that probability and impact can only be calculated using cold hard facts and data.

Chapter 3 is centered on the business, which is what risk assessment and risk management is all about. I discuss how to go about this and how to create pictures of the enterprise to ensure that effective risk management is put in place and becomes a must-have business tool.

In Chapter 4 I discuss what true business risk is, how it can be categorized, the fact that risk is not a one-off occurrence, and how to establish a risk universe for evaluating all risk.

In Chapter 5 I talk about one of the most critical issues in risk management—the ability to do it objectively not subjectively. I talk about utilizing a data-centric approach, why it is necessary, and why doing risk assessment and management any other way really does not track logically.

In Chapter 6 I begin the discussion of how to build a fluid dynamic risk model that is designed to flow with the movements of the enterprise and to keep pace with changes as they occur. I also discuss options that can be utilized to drive the model.

Chapter 7 is an extensive discussion of how to actually build a model with all of the various components included. It talks about how to construct an ERM environment that is absolutely centered on the organization in its day-to-day operations. There are extensive examples given throughout the chapter relative to the concept of enterprise risk management and key risk indicators (KRIs). There are examples for the administrative areas of the organization as well as operational areas.

Chapter 8 discusses the future evolution of the ERM model and why this is absolutely essential to keep the ERM environment vibrant and connected with

the business. Also, the subject of how to make systems self-monitoring from a risk perspective, utilizing advanced tooling, is discussed.

In Chapter 9 I raise the issue of special risk situations and related topics that presents significant exposure to the organization. The two key topics that are discussed in this regard are outsourcing and mergers and acquisitions. In addition, I discuss significantly reducing external audit fees through the utilization of twenty-first-century approaches.

Chapter 10 is the last chapter of this book, and we talk about ownership of risk, extending the impact of the ERM environment, and summarize how to build an automated environment to handle all of your governance concerns.

Another subject that is addressed in this book is the prioritization of risk and risk management relative to internal controls. Internal controls can exist separately and distinctly from the business; however, business risk and the business are inseparably intertwined.

I have finally tired of listening to a bunch of supposed experts pontificate on what they believe enterprise risk management to be, while clearly demonstrating they have not the slightest notion of how it should be done in a manner that yields real business value. This approach actually evaluates and manages risk truly on an enterprise basis, and provides a highly effective business tool as well, while many of the others are financial or administration-centric.

Therefore, do not be surprised or alarmed when I take issue with common practices that have been espoused by very large and well-recognized organizations. I am not trying to be hypercritical nor implying that they are not competent nor unethical. I am simply trying to speak the truth regarding those situations that I believe to be counterintuitive or in some cases unacceptable business practice and a poor use of business resources.

Also, be prepared as the approach used here is different from the norm and as such you will have to expand your thought process and allow yourself to accept something other than the same old recycled ideas, not that recycling is bad, but in this case it is. Keep an open mind and shift your thought parameters and I believe you will find a much better approach to ERM at the end of the day.

I now undertake the task of clarifying once and for all what a common-sense, logically structured, ERM environment should look like and why if implemented properly, it will create a singular, highly effective overriding governance infrastructure.

Thank you for coming along on this journey!

Acknowledgments

IN CREATING THE METHODOLOGIES that underlie this book, even though they are my concepts, I have been fortunate to have the support of some key people. The first person I would like to acknowledge is Joel Kramer of MIS Training Institute, who believed in my talents and my thought processes and never once wavered in his support of me as I worked at honing my skills in the seminar business. This helped me greatly in expanding the tools in my arsenal of risk assessment/management and gave me the opportunity to attain the success I have worked very hard to achieve.

Another is Dave Coderre of Canada who had the vision and courage to take my concepts, implement them, expand on them, and standardize them in his professional career. In addition, he also is an author in his own right and gave me the encouragement I needed to undertake this challenge.

I would also like to extend my sincere thanks to Phillip J. Hatch the president of Ventoro who generously gave of his time to talk with me and his permission to use his data often cited in this work from his in-depth study of offshoring and offshore outsourcing.

Most importantly, my beautiful wife Dina and my children Andrey and Vera who are absolutely critical to my success in every way; I could not do what I do without them and their undying support.

Last, but not least, I want to thank Stacey Rivera of John Wiley & Sons for all of her patience and help in bringing this book to reality.

Contents

CHAPTER ONE

1 Corporate Governance: A Gut Check

THE GREAT SOX FALLACY

One of the key corporate undertakings that undermined and will continue to undermine the success of enterprise risk management (ERM) is Sarbanes-Oxley (SOX). The most amazing thing about the SOX effort was how few of the so-called knowledgeable practitioners that were giving guidance on the subject matter actually understood the salient issues relative to why SOX evolved in the first place. I authored and taught an auditor training class entitled "Sarbanes-Oxley: A Road Map to Compliance." It was astounding to see how misguided the compliance efforts were that were being sold to these client companies as the panacea for all of their problems. It was even more astounding to hear how little people really understood about what the act was intended to do and how their whole focus in life was on Sections 302 and 404 of the act. Some of the key points I tried to explain to the seminar participants were the following:

- The problems that gave rise to SOX in the first place did not start nor would they end in finance.

- The real issues were centered on ineffective operations and the inability to generate a profit.
- When the risks that were present in operations that undermined their ability to operate effectively were not mitigated, then the risk of financial ineptness was imminent.
- This would leave the financial people with no other alternative but to manipulate the numbers to meet analysts' expectations.
- Implementing an overabundance of controls in finance for financial reporting would not solve the problem.
- There were many more sections to the act than just Sections 302 and 404, such as Section 409 on real-time disclosure.
- The gathering up of a bunch of control information and then trying to test them inadequately with archaic methods was going to be of little or no use.
- The preferred method of compliance (a top-down risk assessment approach that would be data driven and holistic to the enterprise) was the only effective way to deal with these problems.
- When the risks were identified, the root causal events had to be addressed, and that would be the first step for resolving these issues.
- I also informed them at that time that they had just seen the tip of the iceberg and that there was much more to follow.

The top-down risk-based approach was supported by the pronouncements from the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) in 2005 when they too observed that the "check the box mentality" of the compliance approach used by virtually all of the large consulting houses had missed the mark of satisfying the requirements of the act.

The subsequent gigantic meltdown of the banking industry brought on by significantly undermanaged risk in the real estate markets speaks volumes about the ineffectiveness of the act and gives us a glimpse of another piece of the iceberg starting to surface.

Sarbanes-Oxley was a noble effort in its intent to protect shareholders' interest; however, the message was lost on the practitioners in their zeal to generate quick profits in catastrophic conditions, which they had had a great hand in creating. The first catastrophic mistake was to embrace the Committee of Sponsoring Organizations (COSO) model as *the* framework for compliance—not because COSO is a bad framework; but since it is internal control-focused, it is clearly audit centric. What was required was a business model, not an audit model. Instead of performing a knee-jerk reaction to the circumstances, cooler

heads should have prevailed and waited for the COSO ERM model (completed approximately two years later), which would have yielded a much more beneficial governance structure.

Unfortunately, so much money, time, and effort was put into the Sarbanes-Oxley exercise, with mixed or less than satisfactory results, that it soured senior management in many organizations from taking on any other major corporate initiatives, which would have included ERM, of course. So now there is great resistance to adopting another environment that appears to be an add-on to the already fractionalized compliance efforts of the organization. Therein lies the tale of woe for ERM and the significant reluctance to embrace it.

THE VISION-CHALLENGED LEADING THE EVEN-MORE-VISION-CHALLENGED

Absent the few independent practitioners (like myself) who are crying out in the wilderness against the multiheaded monsters of the world who keep espousing the same old tune, you don't see many fresh ideas coming out of the large-scale consulting groups. It is the same old process for evaluating risks that has literally been around for years. The process is based upon scoring methodologies, such as one-through-five, or zero-through-three or some other convoluted number combination that is applied to risks, control effectiveness, impact, and other such subject matter.

At the end of these exercises, some type of generic "risk-based" conclusion is inevitably reached, which is normally comprised of a band of green, a massive band of yellow, and a band of red. This is normally followed by some other gyration for refining the process, which involves discarding the high and low scorers, tweaking this, and tweaking that in order to justify an already preordained conclusion. Worse yet, the whole exercise must be repeated every time risk needs to be evaluated on an enterprise basis. This will, of course, be necessary because unlike these static models, risk is not static at all. Talk about the application of AI (artificial intelligence)—these exercises are a classic example, in a very different sense of the phrase.

Why in the world do we have all of this massive computing power, generating terabytes of data that supposedly drives everything in our organization and yet not one of the supposed visionaries from these large consulting consortiums has ever thought, *You know what, maybe we should use data as the basis for risk assessment?* What are they thinking? Or even a more puzzling conundrum is that maybe they're not thinking, and therefore where is their vision?

I cannot possibly imagine a bigger risk than spending millions or billions of dollars being led by supposed visionaries who have no vision.

GOING BACK TO THE FUTURE? HOW *NOT* TO RUN IT

One of the greatest risks plaguing organizations in the past, today, and certainly into the future will be the inability to implement successfully progressive, highly advanced risk-centric systems. The following observations are meant to highlight some of the key areas of concern. I originally conceived "The Dirty Dozen Critical Shortcomings of Application Systems Implementation" as an article for publication. These observations came into existence after years of my own audit experience and reverification of its accuracy with thousands of my audit constituents.

I discussed it with Professor Larry Rittenberg, the current COSO Chairman Emeritus, and we tossed it back and forth with modifications. With all due respect to Larry, who is an extremely busy person, since the results of our discussions were never published, I have reverted back to my original content for the purposes of this book.

In the continuing environment of voracious systems implementation, it is perhaps time to step back and learn some lessons from history. Many of these are not new lessons, but neither have they been learned. In the following sections I will visit some critical shortcomings that continue to hinder our progress in real utilization of the vast systems capabilities that our organizations possess.

SYSTEMIC FAILURE: CRITICAL SHORTCOMINGS OF APPLICATION SYSTEMS IMPLEMENTATION

The "dirty dozen" shortcomings are listed and expanded upon in the following pages. They represent my views of significant risks and areas of failure that are all too prolific in this discipline.

1. Moving to a New Application Platform: What's the Business Reason?
2. Inaccuracy of the Financial Projections and Committed Costs of the System (OOPS!)
3. Failure to Establish a Realistic Timeline That Incorporates All Critical Aspects of Implementation

4. The Phase 2 Syndrome—Never Happens!
5. Failure to Do a Total Systems/Personnel Impact Analysis
6. Implementing a Platform Contrary to the Established Design Criteria
7. Back to the Future
8. ACE (The Awful Consultant Experience)
9. Data, Data Everywhere, but I Can't Answer Your Question
10. SCORE (System-Centric Oversight and Risk Evaluation) AWOL
11. The Dog and Pony Show
12. Getting Cooked by the Boilerplate Contract

Moving to a New Application Platform: What's the Business Reason?

One thing that will guarantee failure to achieve the original objective of a project is when no original objective was established. One of the key questions that the system sponsor should be able to address is the primary business reason for the change.

It is not appropriate to change system platforms just for the sake of change or because everybody's doing it. Each organization is unique in its needs and requirements. As a result, because our primary competitors are moving to a client/server platform does not necessarily mean that the client/server platform is appropriate for us. If a financially viable business reason that necessitates the change cannot be specifically identified and justified, there is no reason to change environments.

The business reason must be critical to the overall success of the organization. It must be clearly justified by returns on investment that warrant the capital expenditures, and it must be vital to meeting the needs of our customers, or carving out a larger share of the marketplace, to name only a few.

Migrating to new systems for no apparent reason is a consummate example of following the crowd no matter where the crowd is going. If the crowd is rushing into a burning building, should we all follow along? A new system is not the panacea for all business ills. In fact, it is probably dealing with a symptom instead of the real cause.

Inaccuracy of the Financial Projections and Committed Costs of the System

If you have ever seen the acquisition and implementation of a large-scale system from start to finish you have almost assuredly seen OOPS, the Overspending Our Project Scenario. This can occur in different forms, some of which

are detailed in the following list. The always popular "let's soft sell the original financial estimates to justify the project to senior management or the board." Simply stated, all of the costs are not included that will be required to make the system a reality. Factors that will be "overlooked" include:

- Long-term technical support
- Specialized consultants or contractors required
- Ancillary hardware that becomes necessary due to primary platform inadequacies
- Additional software that will be purchased by the users to plug the "gaps" in the system (real or perceived)
- Future technological upgrades required, which are inherent to the software (turnkey environment—hardware and software)
- Moving beyond Vanilla when it really needs to be a 40 scoop 30 topping banana split to deliver the baseline requirements of the users
- The *real* life cycle of the system before it requires significant changes to keep pace with business changes
- The business interruption that occurs when new releases of the software are installed and the associated costs
- The hidden costs never accounted for when the users are so dissatisfied with the system that is delivered that they have to buy computers and software to build workarounds that have the desired functionality
- The cost of application support when the flood of user requests for modifications materializes because the system misses the mark so badly
- The cost estimate is simply wholly inadequate and poorly prepared, and fails miserably in contemplating all of the cost that will be necessary

Think about it. When was last time you saw a system of any magnitude come in under its original financial and time projections?

Failure to Establish a Realistic Timeline That Incorporates All Critical Aspects of a System

Where do these implementation dates come from, anyway? It appears that they are rarely in touch with reality and what is required for the system to be fully operational and functioning as originally envisioned. Every implementation date should be grounded in some legal or regulatory issue, or in a defined and justified business requirement.

If the required date is known and cannot be achieved—when exploding the timeline backwards given the resources available or essential lead times

required—another course of action should be explored. The common practice of pulling an implementation date "out of the air" and then tying the CIO's and other related party's bonus compensation package to it runs totally contrary to sound business logic.

The objective of the exercise is not to see how fast the system can be implemented, but how well it meets business needs. Half-baked implementations tied to timelines that have no basis in reason or logic always fail to achieve the key objectives: increased productivity, lower operating costs, better information, and ease of use. In fact, in most instances productivity takes giant strides backwards resulting in more hidden cost to the company or organization.

The Phase 2 Syndrome—Never Happens!

Doesn't it seem that the key features that the business requires or that were critical to the overall satisfaction of user community are never in Phase 1? Why is that? It doesn't really do any good to purchase the most powerful and feature-packed system available, and then fail to implement its primary functionality. The standard phrase that is normally heard when the users ask about the features is "It will be implemented in Phase 2."

Unfortunately, as many disgruntled users and overoptimistic senior executives have learned, Phase 2 is a figment of IT's imagination. By the time this event is raised as an issue, new releases of the base software are out, and the hamsters are trapped on the same hamster wheel for all eternity. If the original intent of purchasing the system was to implement minimal functionality, then save a lot of money, buy a cheaper system with far fewer features, or better yet do nothing—it will be a lot less risky.

Failure to Do a Total Systems/Personnel Impact Analysis

Prior to implementing any system, there should be a total inventory performed of all of the systems and personnel that will be impacted by the new environment. This says by definition that IS/IT is only part of the landscape. The users should, of course, be the primary drivers of the system, though IT normally dominates the project, even though it's a staff function and not a line function (another failure point), and as such the analysis should identify all affiliated and peripheral users of the system.

Failure to perform the appropriate impact analysis on both systems and personnel will virtually guarantee a technological or human rejection of the system once implemented. When the project is first anticipated, it should be mandatory that a thorough and complete impact analysis be performed.

Communication and feedback loops should be established to ensure that vital information is available as necessary to everyone who will experience the impact or, more likely than not, suffer the negative fallout of the project.

Implementing a Platform Contrary to the Established Design Criteria

As we have progressed across the spectrum of systems implementation theory, today we've achieved 180 degrees of separation from traditional viewpoints. The problem is that contemporary theory is rarely, if ever, followed in its purest state, therefore issues arise on a postimplementation basis.

The traditional theory of systems implementation was essentially that the organization would purchase a system that most closely approximated its operations and then modify the system to fit the business. As we know contemporary theory—as advanced by Systems, Applications & Products in Data Processing (SAP) and other similar platforms—is to reengineer the business to fit the software. The unfortunate reality is that most organizations want to embrace the new technology but not the new implementation theory.

As such, new platforms are implemented with old theory. Today's systems are self-contained, highly integrated information flow systems, and they are meant to be implemented in their entirety, a pure state of existence. However, in practice only portions of the new platforms are implemented, instead of in their entirety. And then these partial systems are interfaced to other existing systems in the business. Some of the negative results of mixing the two competing theories include the following:

- Potential loss of data integrity and mistrust of the resulting information that is generated by the system
- Excessive maintenance costs on interfacing
- Customization cost to the original software, assuming it can be performed
- The necessity to update the customized environment at great expense each time a new release of the software is brought out
- Potential need for conversion tables or other intermediate steps to convert the data for use, which are subject to error and extremely expensive to maintain

Back to the Future

How many people do you know who would acquire a brand-new $300,000 house with four bedrooms, three baths, and a two-car garage, and then rip