

---

# Enforcing Business Controls through Greater Visibility

This document is intended for business managers, security professionals and auditors who are interested in managing operational risk by reinforcing their business controls within their enterprise applications. It provides a high-level description of the issues surrounding user access and business controls within these systems.

**Approva Corporation**  
1953 Gallows Road  
Suite 150  
Vienna, Virginia 22182  
[www.approva.net](http://www.approva.net)

approva

---

**© 2003 Approva Corporation. All rights reserved.**

The information contained in this document represents the current view of Approva Corporation, on the issues discussed as of the date of publication. Because Approva must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Approva, and Approva cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. APPROVA MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Approva, the Approva logo, and BizRights are trademarks of Approva Corporation and may be registered in one or more jurisdictions.

The names of products of other companies mentioned in this document, if any, may be the registered or unregistered trademarks of the owners of the products.

Approva Corporation • 1953 Gallows Road • Suite 150 • Vienna, VA 22182 • USA

## Table of Contents

Introduction.....	4
Where did we lose control? .....	5
Changing business environment.....	5
Mergers & acquisitions .....	5
New regulations.....	5
Multiple technologies and many experts .....	6
What are the results of this lack of control?.....	6
Who is affected by this loss of control? .....	6
What is being done today? .....	7
What can be done better? .....	7
Summary .....	8

## Introduction

Right now there is a greater need than ever before for an organization to understand and enforce business controls across their landscape. This is largely due to a sluggish economy, increasing government regulations and a handful of highly publicized corporate scandals. Today, corporate executives face a more skeptical investment and customer community; it is no longer enough to say that you're in control, now you have to prove it.

Proving controls in today's business environment is a challenge. Global 2000 organizations are highly automated. Their core business processes are run by sophisticated enterprise applications for ERP, SCM and CRM. These systems entail the full spectrum of applications from financial, procurement, manufacturing, distribution, sales, and human resources. Many organizations use integrated suites from a single vendor or have chosen best-of-breed solutions and integrate them using EAI solutions. Either way, today's enterprise applications have matured to deliver a great deal of flexibility in addressing and solving complex business processes. This flexibility is manifested in sophisticated internal controls and powerful automation capabilities that enable customers to tailor the applications to fit their unique requirements. The demand for flexibility within the applications has not only increased the usability of the applications but it has introduced complexities into the deployment and management of enterprise applications.

The complexity of these systems can lead to a lack of awareness and understanding of what is really happening within the enterprise application and your business processes. What internal controls are in place, and more importantly what controls are not in place? For example, what controls are in place to handle processing of the receipt of a partial shipment? It is not unusual for clerks in shipping & receiving to override the purchase order to reflect the actual receipt, which seems to make sense to them, but later on results in billing, inventory, and production issues. With the proper information, preventing these problems is a simple matter of restricting their privileges within the application. This lack of awareness does not come from a lack of information within the enterprise application, but it often comes from the difficulty or intricacies of retrieving the proper information when and where the manager needs it. Business managers want and need visibility or awareness into exceptions, violations, and anomalies that occur within the business processes. Too often, these go undetected or detected after-the-fact during an infrequent audit of the system. When we consider what these applications support, including information from financial information and human resources records to line of business data, the cost of improper usage or access to this information can represent a significant cost to the company in terms of business inefficiencies, lost revenue or potential fines.

Some organizations understand the potential for damage is there and are willing to cope with a lack of visibility into their systems except in an emergency basis. Others may dismiss the problem out right, until they are burned in an audit. This may not be the best alternative when failure to properly maintain these systems could lead to government fines based on the Sarbanes Oxley Act as well as corporate embarrassment.

So, many organizations today are looking for new methodologies to help reduce the risk associated with a lack of visibility in their enterprise applications.

### **Where did we lose control?**

Why, then, has it become so difficult to maintain visibility into our enterprise applications, to ensure that the proper business controls are in place, and that the appropriate individuals are performing transactions in these systems? It certainly is not due to a lack of effort by corporations and organizations whose IT staffs are typically burdened with day to day administrative responsibilities. Some of the larger issues that have made it difficult to maintain good visibility into the enterprise application environment include:

- A changing business environment,
- Merger and acquisitions,
- New regulations and policies, and
- Multiple technologies and many experts.

### **Changing business environment**

The fluid nature of business requires that changes to corporate structure, personnel and processes be constantly reviewed to ensure a competitive advantage in the marketplace. These changes impact the usage of the enterprise applications that have been deployed. Making changes to these systems can have impacts that reach beyond a single business process and must be reviewed and tested properly before being implemented. Not only does the investment of time in these procedures take away from an opportunity to review the system, it can also change the way the system must be viewed – changes in controls, rules and role assignments that must be accounted for and analyzed.

### **Mergers & acquisitions**

Another major disruption in the deployment of an enterprise application can occur during the acquisition of or merger with another organization. This process can take months to years to plan and implement as business leaders and IT professionals plan for the consolidation of applications, introduction of new applications, design the proper controls and parameters and roll out the new organization's solution. The difficulties here can affect half of the new organization, or more, as processes and policies are changed around them. As difficult as it is to maintain visibility into a single organization, the period of a merger or acquisition can stifle an organization's ability to view controls across the company.

### **New regulations**

Most companies have defined and enforce their own set of policies and best practices. Many of these companies are also further responsible to protect information and access to sensitive information as mandated by federal and international regulations. For example, the financial industry is faced with protecting sensitive personal and financial information under the Gramm-Leach-Bliley Act while healthcare providers are faced with protecting access to patient information under the HIPAA initiative. Whether exposed to industry-specific regulations such as these or not, laws such as the Sarbanes-Oxley Act of 2002 (SOA) reach across all industries. SOA further promotes the CEO and CFO's

responsibilities for understanding and ensuring that proper controls are in place and are effective. All these regulations present an opportunity for industries to improve visibility within their systems for the good of the public, but they also create the need for new (or improved) controls to be put in place or new penalties to face if these controls are not properly implemented.

### **Multiple technologies and many experts**

The issues of maintaining visibility are further complicated by an environment that supports multiple applications, as most large enterprises do. From the business side of the applications to the technical, in order to support multiple applications most businesses adopted a silo'd approach to management and administration. This practice allows individuals to become experts in their application without the burden or complexities of learning another application. Furthermore, this allows individuals to better exploit the capabilities of each individual application, but it also results in very individualized policies and management techniques. Accessing critical information to monitor controls requires tracking down these experts, getting a data extract or report, and analyzing the results – a process that is different not only for each application, but within each organization. To further complicate matters, in many cases all or part of the data being managed in these applications can span one application to another – should the policies that govern their access really be different?

### **What are the results of this lack of control?**

Government action and corporate scandals have promoted awareness of these issues to a new level. Issues that had historically been left up to the IT department to correct have grown to business and *board level issues*, largely due to the *threat of financial loss and/or public embarrassment*. The difficult economic times that we are in do not allow for a hiccup in the accuracy of financial reporting, let alone a breakdown in the controls that govern the information that is reported. The result is that pressure to maintain compliance is high and that high-powered corporate individuals are more involved and more accountable for their organization's actions.

### **Who is affected by this loss of control?**

As with most business issues, the larger the organization the more likely they are to be experiencing a loss of control due to a lack of visibility. There's more to it than simply the number of people involved, however, as each of the following issues creates complexities and reduces our visibility into application data. An organization with one or more of the following characteristics is likely to face higher operational risk due to the complexity of their operations and the lack of visibility into their business processes:

- **Complex organizations** – These large businesses are typically geographically diverse, with a large number of employees, customers and partners. They typically derive a competitive advantage from a close integration with a number of diverse partners. Examples include retail, distribution, services, and government.
- **High risk environments** – These environments are created in industries that are heavily regulated with potential for significant financial, operational and

reputation penalties for non-compliance. Because of the heavy burden on the internal and external auditors, these businesses may find themselves in reactive mode versus proactively eliminating threats. Examples include healthcare, insurance, financial, and pharmaceutical.

- **Complex business processes** – These organizations rely on complex supply chains and close supplier support to ensure their business runs in a timely and proper manner. Examples include discrete and process manufacturing.

### ***What is being done today?***

Maintaining control over these types of environments is an enterprise-effort. To one degree or another, nearly every employee of an organization is responsible for defining or carrying out the processes and controls that the company has put in place to ensure that the organization's best interests are met. Of course, if rules are meant to be broken, then someone must watch for violations; violations that can often lead to a loss of money or reputation within the industry.

Given the issues Corporate America is facing in today, there has been a significant effort to re-focus and re-emphasize the importance of understanding what is happening within an organization. Again, the Sarbanes-Oxley Act emphasizes this concern as corporations are further tasked to ensure the accuracy of their financial reporting. A key aspect of this commitment is to ensure that the proper internal business controls are in effect and that they have been followed. This, in turn, has led to a significant effort on the part of a number of groups and individuals who are tasked with getting these issues under control. Driven from the Audit Committee of the Board; internal audit groups, external auditors and software tools are working to achieve this goal.

Through a combination of manual verification, random spot checks, time-consuming audit reviews and ad-hoc verification of information these groups face an often insurmountable task of digesting large volumes of data. Today's software tools enable auditors of all kinds to explore data and get to the cause of suspected issues. However, what's missing is the ability to proactively monitor for exceptions, violations, anomalies, and conflicts.

### ***What can be done better?***

As long as compliance is viewed as an 'audit' issue, organizations will face time-consuming and expensive auditing procedures as they try to maintain control over the information in their organization. While controls are established and manual efforts are made to ensure they are carried out, lack of time, resources, training or any other number of personnel issues can lead to an imperfect record when it comes to adhering to the policies at hand. Paper-based processes and the complexities of large, distributed organizations can further compound this problem.

To add to the lack of visibility, over the next couple of years we will see a number of web service based or enabled applications that will further promote communications between applications and across organizations. This is necessary to meet the expanding needs of industry, but is not without the burden of increased volumes of information.

The manual processes that are employed today cannot scale effectively to meet this new volume of data.

To meet the needs of today's and tomorrow's applications, then, a solution must look at prevention as well as a cure. Manager's and IT groups must continue to be empowered to manage usage of their applications, but they need visibility into the regulations and policies that they must follow at the time of assigning access to their employees. The days of relying on a piece of paper to define policy may be numbered and it is important that these solutions prevent issues such as Separation of Duties from ever occurring. Managers must know that policies are being followed, and if something has gone wrong, they need to know when it happens. Organizations need visibility into how their business applications are being used, who is using them and who allowed them to use the applications in the first place. Only through a continuous process can information be provided in a digestible size and in a timely fashion to allow management to prevent unwanted activity today.

## Summary

Complex business problems have created complex applications for managing information. The number of people, processes and technologies that are involved in using these applications has clouded many organization's visibility into the proper usage their systems. To further complicate matters, government, industry and organizational policies that define proper usage are changing; they are increasing in scope and are more pervasive than ever before. In many cases the level of control has dropped to a point where organizations are uncomfortable with their ability to properly control their business on a day-to-day basis. It can be better, though; the question is *what* can be done better?

The key to gaining control is **visibility** into the management of application usage, **visibility** through analysis of the transactions that take place and **visibility** into the exceptions that are found. Organizations need *greater visibility* into these applications in order to maintain *better control*.

