

COMPLIANCE

Help Achieve Compliance Objectives with Microsoft Dynamics GP

White Paper

Date: June, 2006



Table of Contents

- Introduction 3**
- Compliance Defined 3**
- Sources of Compliance Requirements..... 4**
 - Government Compliance Requirements..... 5
 - Food and Drug Administration..... 6
 - Industry Groups 7
- Operational Requirements for Compliance 7**
- Compliance Concepts 8**
 - Processes 8
 - Standard Operating Procedures..... 8
 - Documented Transactions..... 8
 - Data Integrity..... 9
 - Audit Trails..... 9
 - Separation of Duties/Responsibilities 9
- Technologies to Support Compliance Requirements 10**
 - Technologies..... 10
 - Workflow 10
 - Audit Trails..... 10
 - Electronic Signatures 10
 - Compliance Program Matrix..... 11
 - Compliance Control: Prevent and Detect..... 11
- Compliance Management in the People-Ready Organization 11**
 - Designing Your Compliance Management Program 12
 - Executing Your Compliance Management Program..... 12
 - Compliance Management and the People-Ready Organization..... 13
- Summary 13**
 - About Microsoft Dynamics™ GP 14

Introduction

The demands placed on executives to balance compliance requirements with those of stockholders and the market has increased dramatically over the past few years. In the face of laws such as Sarbanes-Oxley, along with increased scrutiny of long-standing government compliance requirements following a rash of corporate scandals, executives are challenged with the seemingly contradictory goals of compliance adoption and organizational agility. Compliance adoption brings highly structured processes and rigidity to activities, while the goal of organizational agility is to drive innovation, develop and expand customer relationships, improve operations, and build stronger business relationships. Balancing the rigidity of compliance with the flexibility that allows people to create a better and growing organization can be achieved through better understanding of compliance requirements and how they are integrated into business process systems that are people-ready and designed for agility.

The objective of this document is to provide company executives and mid-level managers who are facing compliance requirements with guidance in implementing and maintaining compliance processes while maintaining and/or enhancing the agility of the organization. This document will assist you in:

- Understanding the meaning of compliance
- Identifying the sources of compliance requirements
- Understanding the operational requirements of compliance and their integration into Standard Operating Procedures
- Implementing compliance requirements while maintaining an agile, people-ready organization

By actively managing the integration and balance of compliance requirements and agile business practices within the organization as a business improvement activity, businesses can realize the benefits of reduced risk, increased operational efficiency, and the continued building of a foundation on which to grow.

Compliance Defined

The simplest definition of compliance is observance, conformity, and obedience. In business, compliance generally designates the requirement to adhere to certain rules/laws, meet certain standards, and follow certain practices. Compliance standards can originate from external as well as internal sources. A compliance requirement may be mandatory or optional.

Understanding the origin of compliance requirements enables appropriate prioritization and risk management. Compliance requirements that your organization must adhere to may be based on your ownership structure, management practices, location(s), and the market(s) in which you wish to participate, as well as your specific industry, customer, and vendor affiliations. Later in this document we will explore the sources of compliance requirements and provide public domain references to assist you in researching their specific requirements. If you look at your business practices, you will see that many standard operating procedures exist to satisfy the compliance requirements of all the entities, internal and external, with which the organization interacts.

Today the majority of compliance requirements focus is around Government-imposed regulations, and perhaps rightfully so because of the real possibility of civil and criminal penalties directed to top level management in the case of breach of compliance. But in the rush to comply with government regulations,

management must not lose sight of the compliance standards (whatever their source) that the organization is already complying with and why they are complying with them.

Questions that ownership and management must continually consider:

- How do all of the compliance requirements get managed within the operational structures of the organization?
- How are business structures and operating practices enhanced when adopting compliance practices while maintaining profitability, market share, and organizational agility?

Sources of Compliance Requirements

Compliance requirements are nothing new to business. Customers, vendors, and governments have always provided businesses with standards for interaction. From tax reporting forms to how you place a label on a box for a customer, compliance requirements drive businesses to accomplish things in very specific ways. So, to really understand compliance requirements for your business you need only look around at the ways you accomplish tasks (especially repetitive tasks), communicate, and keep information, and then ask “Why?” The answers will point you to the source of a compliance requirement.

Compliance requirement sources are not only external, for example from the government, customers, and vendors, but internal as well, from owners/management, investors, and other departments. Although the internal compliance requirements may not seem as pressing, they often provide the greatest business optimization opportunities. For example, management may require that along with recording a customer product return, a reason for the return must be recorded. This additional data capture adds additional steps for the receiving department initially, but in the long run, knowing why an item was returned assists management in making adjustments to marketing, sales, production, quality control, purchasing, shipping, and so forth, helping reduce any further returns. In the long run, this reporting and corrective action process obviously has significant positive financial impacts for the organization. As you examine internal compliance measures, consider using compliance requirements to more closely manage things that represent high risk and/or high value to the organization, such as environmental impacts caused by operations or product spoilage or damage caused by equipment failure.

To assist you in locating the sources of compliance in your organization, the following list outlines potential internal and external sources of compliance requirements:

- Internal
 - Ownership
 - Stockholders
 - Internal Audit Committee/Board
 - Management
 - Legal
 - Other Departments
- External
 - Government

- Banks
- Customers
- Vendors
- Partners (legal, insurance, real estate, etc.)
- Industry Groups

External compliance requirement sources have the extra burden of often being mandatory, strict in implementation structure and reporting requirements, and typically have legal and financial implications. Recent focus on compliance has been with regard to external legal and financial compliance requirements originating from Government regulations. For example, by law, many public organizations had to rapidly implement Sarbanes-Oxley requirements. Within the private sector, pharmaceutical and food companies have long understood quality assurance and track and traceability requirements.

The following information provides some direction to assist you in the finding, gathering, organizing, and documenting some of the government compliance requirements that are the most pressing and relevant to businesses today.

Government Compliance Requirements

Governments seem to have an endless flow of regulations directed at businesses and provide the business community with the greatest challenges to compliance. Many regulations target specific industries and businesses, while some apply to all businesses. Government compliance regulations reach across the entire spectrum of business operation activities – from tax collection and reporting, to manufacturing quality verification and material tracing capabilities, to corporate governance. More recently, some of the most pressing government regulations stem from the emergence and adoption of computer data and transaction systems and corporate governance. The transformation from “paper tracking” and its associated paper trail to the use of data systems and the potential lack of transaction trails left a gap in the government’s ability to inspect and regulate things such as drug manufacturing processes. Corporate governance has become a hot topic because gaps in disclosure to stockholders and the public were highlighted through the spectacular failure of several organizations with little or no warning.

There are over 60 regulating US government Agencies that issue compliance regulations (see www.regulations.gov). Depending on your business, you may be required to adhere to one or many of these regulations across multiple agencies. For example, a publicly traded pharmaceutical company would be required to adhere to various SEC and FDA compliance regulations.

Securities and Exchange Commission (SEC) and Sarbanes-Oxley

Sarbanes-Oxley requirements were enacted by the United States Congress as a reaction to a string of surprising corporate failures and scandals. The act required that all relevant audit-related documentation be retained for a period of at least seven years. This includes contracts, policies, authorizations, verifications, recommendations, performance reviews and financial data. Anyone who knowingly alters, falsifies, destroys, or otherwise tampers with a document or record can be fined and/or imprisoned for up to 20 years.

Sarbanes-Oxley was enacted "to improve quality and transparency in financial reporting and independent audits and accounting services for public companies, to create a Public Company Accounting Oversight Board, to enhance the standard setting process for accounting practices, to strengthen the independence

of firms that audit public companies, to increase corporate responsibility and the usefulness of corporate financial disclosure, to protect the objectivity and independence of securities analysts, to improve Securities and Exchange Commission resources and oversight, and for other purposes."¹ (See <http://www.sarbanes-oxley.com/section.php>)

As directed by the Sarbanes-Oxley Act of 2002, the SEC is adopting rules that require conformance with specific sections of the Act. These rules require officers to certify that they are responsible for establishing, maintaining, and regularly evaluating the effectiveness of the issuer's internal controls; that they have made certain disclosures to the issuer's auditors and the audit committee of the board of directors about the issuer's internal controls; and that they have included information in the issuer's quarterly and annual reports about their evaluation and whether there have been significant changes in the issuer's internal controls or in other factors that could significantly affect internal controls subsequent to the evaluation.²

Food and Drug Administration

The FDA's mission as a public health protector includes ensuring that "human and veterinary drugs are safe and effective; that there is reasonable assurance of the safety and effectiveness of devices intended for human use."³ Today, the need to audit processes concerned with human health has become even more critical in light of current bioterrorism fears.

The FDA has defined Good Manufacturing Practices (GMPs) to ensure that Life Science products are produced in a manner that supports its mandate. Originally, GMPs were based upon the best practices of the industry. As technology and practices improved, the GMPs evolved as well. GMPs for the U.S. drug industry were formally introduced in 1963 and were significantly rewritten in the 1970s. GMPs define a quality system that manufacturers use as they build quality into their products. For example, approved drug products developed and produced according to GMPs are safe, properly identified, of the correct strength or potency, pure, and of high quality. At a high level, GMPs provide guidelines for:

- Properly designed, maintained, and cleaned equipment and facilities
- Documented Standard Operating Procedures
- An independent Quality unit (such as Quality Control and/or Quality Assurance)
- Well-trained personnel and management

¹ FDA Mission Statement. See - <http://www.fda.gov/opacom/morechoices/mission.html>

² See <http://www.fda.gov/cder/dmpq/cgmpregs.htm> for current regulations.

³ FDA Mission Statement.

Good Manufacturing Practices (GMPs) are defined as regulations that describe the methods, equipment, facilities, and controls required for producing. These regulations are found in the Congressional Federal Register (CFR) 21 in the following parts:

- Human pharmaceutical products and veterinary products (21 CFR 210-211)
- Biologically derived products (21 CFR 600 and 21 CFR 620)
- Medical devices (21 CFR 820)
- Processed food (21 CFR 100)²

Industry Groups

Like governments, prominent industry organizations have the power and arguably the responsibility to use their influence to assure the protection of their interests, whether they are human safety and health, and/or financial security. Industry organizations therefore often create a set of guidelines and rules to provide reasonable assurance of safety and effectiveness. An added benefit of organizations becoming more actively involved with the industry groups most closely aligned with their business operations is that the industry groups are a good source for assistance in knowing and understanding the compliance requirements your organization must adhere to.

Getting a complete understanding of the sources of compliance for your organization will enable you to appropriately plan ahead and efficiently adopt and retire compliance requirements as the requirements and your organization evolve. The next focus for compliance management then becomes: “How do I adopt a new, strict structure of compliance requirements and keep current compliance actions intact while enhancing the organization’s profitability, its abilities to innovate, adapt, and optimize?”

Operational Requirements for Compliance

Compliance requirements force change in the way people approach and accomplish tasks, the data that is captured through conducting activities, and the way and timing that the information is consolidated, presented, and disseminated. Understanding what tasks are affected and what information about the task needs to be captured provides guidance to what is needed to comply with that specific requirement. Reviewing the many compliance requirements, it can be seen that they impact the following aspects of a business:

- Design standards
 - Performance standards as dictated by the compliance requiring organization.
Example: The fuel-filling point for an aircraft must be such that fuel does not siphon out of the tank during flight in the event the gas tank cap comes loose or is missing.
- Quality standards
 - That the products maintain a certain quality (sometime purity)
Example: A finished pharmaceutical must not contain any unwanted material or microbes.
- Process
 - The method in which the activity, product, or service was executed, created, or delivered follows a set standard.

Example: Prior to shipping product to a customer, an Advanced Shipping Notice (ASN) Electronic Data Interchange (EDI) must be sent to the customer.

- Reporting
 - The assurance that sufficient and appropriate data is captured and disseminated in an appropriate and timely manner.

Examples:

Traceability (materials, activities, personnel, financial)

Financial (tax, significant events)

Compliance Concepts

Processes

Even though there are many ways a compliance requirement can impact a business through changing its business processes and/or changing how and where data is captured, the categories of compliance requirements are fairly limited. Identifying and understanding a compliance requirement's relative categorization assists in selecting the correct set of process and technology solutions to assure compliance. Compliance requirements fall into the following categories:

- Standard Operating Procedures
- Documented Transactions
- Data Integrity
- Audit Trails
- Separation of Duties/Responsibilities

Standard Operating Procedures

A Standard Operating Procedure is typically instituted within a business to provide efficiency, consistence, standardization or action, and is also used as a tool to assist in the training/execution of new people executing any particular function or task. With compliance, Standard Operating Procedures are added or adjusted to meet the requirement. For example, a pharmaceutical manufacturer that has a clean room manufacturing environment must create Standard Operating Procedures for the actions a person takes when entering the clean room environment. This may include a shoe cleaning station and the usage of shoe covers. Ensuring that this step-by-step Standard Operating Procedure is created and made available, clearly accessible, and readable at the clean room entrance could be only one of many points in meeting the compliance requirement of assuring product sterility.

Documented Transactions

Many compliance requirements are simply to record exactly what happened, when, and by whom. For compliance requirements that require Documented Transactions, the transaction should be captured as close to the source of the transaction activity as possible. For example, a sausage manufacturer must be able to track meat products from their origin to completed products. The receiving function should record

the receipt of the data – meat product and the associated lot, vendor, date, time, received by, and so forth – as the item is received. Then, as the product is pulled from inventory and placed into production, additional data must be captured showing that this raw meat lot was issued to make a particular lot identification of a product as the item is picked, and so on until the item is shipped out the door. Having this data provides an information chain back to the original raw material, along with the ability to inspect and/or quarantine any associated products or raw materials up or down the production chain if any issues of quality or safety arise.

Data Integrity

If you document transactions electronically to meet compliance requirements, there must be assurances that the data is available, secure, and tamper proof. In cases of sensitive data such as credit card and Social Security information, this is a must, and the organization may face significant risk and financial implication if this data is mismanaged. To assure data integrity, systems and procedures must be put in place to ensure high availability, such as backup processors and disk systems, data encryption within your systems and for any data that gets transmitted, sent, or stored on remote storage media that has any potential of ending up in unintended hands.

Audit Trails

Documenting transactions and capturing and securely storing data is often not enough to meet compliance requirements. There must also be a trail of exactly what changes happened to the data, when it changed, and who/what made the change. This trail of changes is typically referred to as an audit trail. For example, the credit limit of a customer is often a data point that is required to be controlled by corporate governance compliance requirements. Each time a customer's credit limit is changed, the audit trail will record the old credit limit, the new credit limit, the date and time the change was made, and what user made the change. Having this information makes it possible for management and auditors to see that credit limits aren't being improperly manipulated by sales to process orders for customers who may provide accounts receivable risk to the organization.

Separation of Duties/Responsibilities

With highly critical decisions that carry high risk/high value, it is often not advisable to place such significant risk and responsibility in the hands of a single individual. In a chain of related processes, this means separating the authority of people to manage only sub-sets of activity, where to complete the entire process takes two or more people. This is the case when processing payments to vendors. There should be people who have the authority to enter purchase orders (POs), approve the receipt of the materials/services, and enter the vendor invoices and match them against the POs, and someone completely different approving and delivering payment. Having this separation helps to eliminate payment for goods/services not approved and/or actually delivered.

Often separation of duties is not enough when managing data transactions. In this case a two-deep approval to change data or record data is required to secure against fraud and/or minimize entry errors. In such situations the systems should not accept the data entry until a second individual gives their approval. This is often the case when changing a critical parameter such as formulation in an item's bill of material for a pharmaceutical.

Technologies to Support Compliance Requirements

Technologies

Technology solutions have matured rapidly over the past several years to support compliance requirements. These tools are now readily found to be completely integrated into Enterprise Requirement Planning (ERP) systems. There are several modules, or components, within ERP systems that are critical to managing compliance requirements. They include:

- Workflow
- Audit Trails
- Electronic Signatures

Workflow

Applications that enable workflow and integration with communication systems provide a structure for managing Standard Operating Procedures, where multiple people and complex interdependencies exist. Workflow can be used in the situation discussed above where a formulation change is being suggested for a pharmaceutical. When such a change is proposed, there are many departments and individuals that have to be notified and given the ability to provide feedback and concerns. So, if the development laboratory makes the request for the change, the change request has to be sent to engineering, production management, material management, purchasing/vendor sourcing, quality control, and so forth. Having a system manage the distribution and consolidation of all feedback can not only save a lot of time, but also can provide assurance that all who needed to be notified were notified and gave their specific sign off.

Audit Trails

Audit trails solutions track the markings of all critical transactions. These solutions constantly monitor minute data changes and record details about the change. Audit Trail capability will be required by compliance auditors so that they can review the integrity of data and see the specific change history information for certain significant transactions. In order for audit trails to be reliable, they must be complete. This includes the ability to monitor changes to the data regardless of the source of the change. A true Audit Trail solution will capture data changes whether their source is an application system or a database administrator using a data manipulation tool.

Electronic Signatures

A key approach to the separation of duties is having technology solutions that require two-deep sign-off on critical data changes or transaction entries. Electronic Signature solutions typically require that during the data transaction, a second "approving" individual must inspect the transaction and provide their electronic signature, typically in the form of user id and password. Electronic signature applications may also use biometrics to capture approval to guard against password sharing. In these systems, the biometric ID is provided through a physical interaction with the computer such as a fingerprint read. Fingerprint, retina, handprint, or other forms of biometric input are often referred to as digital signatures.

Compliance Program Matrix

A clear delineation of process requirements and their supporting technologies assists in keeping the implementation of a compliance program appropriately focused. Often the use of a Compliance Log is used to manage all the requirements that the compliance officer or manager is responsible for. This living document can assist in ensuring that:

- Compliance requirements are being met and managed.
- The organization efficiently adopts new compliance requirements while assuring that efforts are not duplicated.
- High level documentation is provided in cases where compliance tracking activities are canceled for whatever reason.

Some things to track in the compliance Matrix Log:

- Risk Assessment
- Requirement origination
- Responsibility
- Processes
- Supporting technologies
- Reporting/recording points

Compliance Control: Prevent and Detect

Compliance requires organizations not only to prevent inappropriate activities and transactions but also to have so-called "detect" mechanisms in place to timely identify activities/transactions that fail the requirements. The exact detect mechanism and detect frequency is based on the risk assessment of the certain compliance requirement. Extremely high-risk compliance points should have an almost immediate detect mechanism in place, while low-risk compliance points may have monthly, or quarterly detect mechanism. A detect mechanism may be automated – for example, through system logic that identifies when a piece of data falls outside a certain range, or through an audit trail record. Detect mechanisms also can be manual – for example, transaction/process reviews by an auditor. The result of a non-compliance detect would be a non-compliance report and a corrective actions process with appropriate reporting to your organization's Audit Committee, so that they may determine if this non-compliance requires additional reporting to internal and/or outside organizations.

Compliance Management in the People-Ready Organization

A people-ready organization automates routine tasks and provides real-time information so people can make timely decisions with increased confidence. A goal of a people-ready organization is to enable people to focus on activities that add the most value. Yet initiating a compliance program can feel intimidating to your people. It typically involves changing business processes that affect many people and adding responsibilities and tasks to their already overloaded schedules. At the same time, a successful compliance program typically does improve business performance and reduce organizational risk.

Managing the interrelationship between business goals, personnel, compliance requirements, Standard Operating Procedures, organizational agility, expansion (or shrink), continual process improvement, product quality, innovation, service, and other factors in your business is critical to long-term organizational success. The following provides some points/steps to examine within your organization to provide healthy and long-lasting balance when considering compliance requirements in relation to other factors.

Designing Your Compliance Management Program

1. Establish a compliance board.
 - a. Chief Compliance Officer (CCO) chair, Departmental heads as members
2. Document all compliance requirements in relation to the short, mid, and long-term goals and objectives of the organization.
3. Understand and document the strategies of each department to meet their compliance objectives.
4. Understand and document the procedures of each department's compliance processes.
5. Document and understand the relationship between each department within the procedures of the compliance program. (consider graphical charting or processes and relationships)
6. Identify risks (legal, financial, operational, market perception, other) and corresponding compliance requirement points.
7. Relate the compliance requirements to standard operational procedures, data, personnel authority, security, audit, and sign-off requirements.
8. Identify how a compliance action affects other processes, and departments.
9. Determine if there are significant additional actions or considerations (Standard Operating Procedures, policies) that need to be examined.

Executing Your Compliance Management Program

The following points are offered to help achieve compliance within your business while maintaining the benefits of a people-ready business.

1. Communicate the overall compliance program with department management and key employees.
2. Encourage and facilitate teamwork by using the appropriate enabling technologies.
3. Categorize compliance requirements into groups and designate what functional areas they impact.
4. Identify the point(s) in which the compliance measure will be integrated into business systems and Business Operating Procedures.
5. Set responsibilities and rules on how compliance procedures and data are to be managed.
6. Establish the criteria for maintaining and managing the relevant compliance procedures and data.
7. Communicate and document guidelines to ensure all involved people know the legal and financial consequences of compliance process mis-management.
8. Provide for non-compliance reporting and corrective action documentation.

9. Utilize procedures and systems to manage exceptions and encourage people to provide insights to enable compliance process improvement.
10. Seek and build strong relationships with external resources that can provide expertise on compliance areas that are relevant to your business.
11. Create Standard Operating Procedures for personnel to follow; include the exception processes.
12. Enable and support data capture, audit ability, security, backup, and archiving in your compliance processes.
13. Document all data retention requirements.
14. Set procedures and the ability to audit all data deletion with two-deep sign-off when data is deleted if required based on risk assessment.
15. Set compliance responsibility at the executive officer and manager/director levels of the organizations. Instill expectation within all employees that they are responsible to execute upon the defined compliance policies. If the policies are not clear or there is question about their applicability in a situation, have a defined compliance issue escalation process.
16. Institute a continual compliance review and improvement program. Utilize compliance Key Performance Indicators (KPIs), people insights, exceptions, non-compliance data and external monitoring of compliance regulations as feedback to improve processes.

Compliance Management and the People-Ready Organization

As discussed in the sections above, compliance affects set business operations and/or reporting points in your business processes. Agility is enabled by building the following characteristics into your compliance program, allowing your people to focus on tasks that add the most value:

- Empower people to be innovative and provide insights.
- Include a method for people to categorize and deal with exceptions.
- Institute a process to record non-compliance and corrective actions.
- Use a system that enables people to quickly and effectively communicate.
- Use a system to continually monitor, evaluate, and improve processes.

Summary

Knowing what compliance rules you need to live by, where they originate, and where they impact your people and business helps you implement compliance management solutions in a way that actually improves business operations while managing risk and meeting compliance requirements. In addition, the solutions and processes that you make available to your people to manage exceptions and quickly and effectively communicate information can provide your organization with a foundation for continuous business improvement.

Continuous business improvement depends on giving your people information to make informed decisions. Compliance requirements often force the capture and retention of key information, such as exception and nonconformance feedback from your employees and auditors. Successful organizations will utilize these feedback loops to become more efficient, create more functional and higher quality products

and services, and to create new and differentiating advantages in the value they offer to customers. Using information technology, people, and processes to enable compliance management in a "People-Ready Business" can create short-term and long-term prosperity for your organization.

About Microsoft Dynamics™ GP

Microsoft Dynamics GP provides the framework and tools to help businesses manage the challenges of compliance. Microsoft Dynamics GP, combined with the expertise of our consultants and partners, offers a full solution set, of software and services that empower businesses to:

- Increase control and reduces the cost of compliance processes.
- Increase the efficiency of the compliance process
- Help manage the risk of compliance processes

Increases control and reduces the cost of compliance processes

Microsoft Dynamics GP offers an automated approach to compliance that helps increase controls through data integrity and data security and helps reduce the cost of compliance processes. In addition, by extending your current Microsoft Dynamics solutions in ways that fit seamlessly with your existing IT architecture, you can help accelerate deployment and minimize IT costs.

1. Data integrity helps you to prove that your data is trustworthy and that it has not been tampered with.
 - a. Track, trace and report changes to any Microsoft Dynamics GP data fields and tables relevant to your compliance strategy with Audit Trails for Microsoft Dynamics GP.
 - b. Safeguard historical information on the actual performance of regulated processes and recreate and compare transaction history, including time, date, and user, as well as before change and after change data values with Audit Trails.
2. Gather approval information electronically and store it for later verification and history review to ensure necessary data security is in place.
 - a. Set up compliance control processes centrally in the system so they are automatically activated during the actual performance of the business process with Electronic Signatures in Microsoft Dynamics GP. This module enables two-deep sign-off approval with reason code and comment capability that is fully integrated with Audit Trail functionality in Microsoft Dynamics GP to monitor the details of changes and approvers.
 - b. Control access to data throughout Microsoft Dynamics GP by managing security restrictions on individual data fields, windows and forms. Define how you want security restrictions managed and assign those rights.

Increases the efficiency of the compliance process

By providing an automated approach to compliance, Microsoft Dynamics GP can help increase the efficiency of the compliance process and can improve business performance because processes can be performed faster, with fewer people, and with higher levels of control, using systems that share information across your organization and are familiar and easy to use.

1. Deliver Data Security through user defined and centrally managed controls to eliminate manual processes and the possibility of human error.

- a. Obtain approval information for user-defined compliance control processes electronically with Electronic Signatures and store it for later verification and history review by Audit Trails.
 - b. Improve management and gain greater reporting flexibility and extensibility by instituting controls on your Chart of Accounts with Analytical Accounting in Microsoft GP.
 - c. Ensure the lockdown of budget numbers and pre-defined approval hierarchies that limit who can participate and who has final approval with Microsoft Forecaster.
 - d. Filter account views by granting user- or class-level access with Account Level Security in Microsoft Dynamics GP, which increases security and eliminates errors caused when entries are made to inappropriate accounts.
2. Automate compliance processes to free up people to focus on the activities that add value to your business, rather than disrupting workflow through manual tracking for compliance processes.
 - a. Minimize user training requirements with software systems that are familiar because they work like and other Microsoft® Windows® applications you already know. People can get up to speed quickly and focus on their area of expertise without spending time learning a new software application.
 - b. Ease the IT burden with compliance modules that are centrally managed and share a common database, helping reduce the need for additional background systems processes and activity.
 - c. Increase auditor and internal confidence through familiar tools that are dependable and easy to use, freeing up people's time and energy for work that's more important than going to training and checking the manual.
 3. Respond rapidly to the changing demands of your business with more complete insight across your organization that empowers people to make timely and informed decisions with increased confidence.
 - a. Enable cross-functional collaboration and help teams and divisions stay on the same page by sharing a common set of data across all systems and users.
 - b. Facilitate documentation and evaluation of controls with Business Portal in Microsoft Dynamics GP: Share compliance updates and increase employee productivity by providing role-based access to a common set of shared data and processes across all systems and users from a single Web-based portal.

Meet business objectives and gain competitive advantage with budgeting and planning capabilities that allow you to take more control of the process, readily adjust to changing conditions and develop more realistic and accurate budgets with Microsoft Forecaster.

Helps manage the risk of compliance processes

By delivering an automated approach to compliance, Microsoft Dynamics GP helps you manage the risk of compliance processes. Deep functionality equips you to enforce Standard Operating Procedures, and can eliminate errors associated with manual compliance processes through integrated, dependable applications and information systems.

1. Reduce risk by preventing errors that could occur at pre-configured control points, while maintaining speed and efficiency for the business processes requiring these types of controls.
 - a. Contain risk by pre-configuring Microsoft Dynamics GP to require multiple passwords that indicate the authorized signers' approvals before controlled changes are allowed to proceed with Electronic Signatures in Microsoft GP.
 - b. Because Microsoft Dynamics GP operates with Microsoft Windows 2003 and Microsoft SQL Server™ 2005, Electronic Signatures extends the single point of authorization for enforcing strong passwords and strong password procedures already in place.
2. Gain visibility into KPIs by increasing data accessibility so you can anticipate business situations that may benefit from early intervention, helping ensure that your business meets requirements proactively, rather than simply reacting to crisis.
 - a. Develop more realistic and accurate budgets based on a single, unique data set with financial data drill-down capabilities and easy data access
 - b. Define information that is important to your business and analyze financial data using your own criteria with Analytical Accounting in Microsoft Dynamics GP.

Microsoft Dynamics GP delivers an integrated and automated solution designed to help you manage the risks and costs associated with meeting compliance requirements, extend your investment in Microsoft products and technologies, and give you deeper visibility into and control of business practices that you can use to generate a competitive advantage.

Microsoft Dynamics is a line of integrated, adaptable business management solutions that enables you and your people to make business decisions with greater confidence. Microsoft Dynamics works like and with familiar Microsoft software, automating and streamlining financial, customer relationship and supply chain processes in a way that helps you drive business success.

U.S. and Canada Toll Free 1-888-477-7989

Worldwide +1-701-281-6500

www.microsoft.com/dynamics

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

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved. Microsoft, Microsoft Dynamics, the Microsoft Dynamics Logo, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States or other countries.