DELIVERING IT CONTROLS FOR SARBANES-OXLEY COMPLIANCE

Financial accounting and business management systems are integrated in the initiating, authorizing, processing, and reporting of financial data and therefore need to be assessed for compliance with the Sarbanes-Oxley Act of 2002. This document discusses the specifics of the Sarbanes-Oxley Act that are relevant to financial accounting and business management systems and then describes how Microsoft Dynamics™ GP can support these requirements.

Background

The Sarbanes-Oxley Act of 2002 is widely regarded as the most significant securities regulation to affect companies since the passage of the Securities Act of 1934. At present, approximately 15,000 listed companies with a market value in excess of $37 trillion USD are affected by the Act. Since 2002, Sarbanes-Oxley or similar, harmonized regulations have been in effect in the United States, Canada, Britain, France, and Japan (pending). The European Union (EU) has passed the updated Eight Company Law Directive, which requires strong internal controls for all listed companies within the 25 EU member countries.

The Act contains eleven titles, or sections, ranging from additional corporate board responsibilities to the creation of a new agency, the Public Company Accounting Oversight Board (PCAOB), responsible for overseeing accounting firms in their roles as auditors of public companies. The PCAOB also provides guidance on the internal controls framework companies must use to comply with the Sarbanes-Oxley Act and on the role of IT controls in this process. The Sarbanes-Oxley Act makes it a criminal offense for officers of a company to willfully submit financial reports that are known to be inaccurate. Moreover, the Act makes it a criminal offense for a company officer who has had sufficient notice of financial reporting problems to deliberately refuse to recognize or act on that information.

IT Controls

According to the internal controls framework referenced by the PCAOB (Auditing Standard No. 2), auditors must make an assessment as to whether a company has put in place controls (including IT controls) that not only detect errors but also detect and deter fraud. To comply with Sarbanes-Oxley, an organization must understand how the financial reporting process works and identify the areas where technology plays a critical part. Organizations also need to recognize that technology controls can have a direct or indirect impact on the financial reporting process. For example, application controls ensure the completeness and accuracy of the transactions that become directly related to financial reports. Application controls are usually aligned with business processes that produce the data that goes into financial reports. Access controls are equally important, because they have an indirect effect on the accuracy of the financial reports. Access controls may reside within the applications, databases, networks, operating systems, or supporting systems that contribute to the financial reporting function.

Enabling IT Controls for Compliance using Microsoft Dynamics GP

The Sarbanes-Oxley Act contains four sections that result in the need for IT controls, including application controls and access controls:

302: Corporate Responsibility for Financial Reports

404: Management Assessment of Internal Controls

409: Real-Time Issue Disclosure

802: Criminal Penalties for Altering Documents

Below is a brief description of each section, a summary of the IT controls needed to support compliance with the section, and an explanation of how Microsoft Dynamics GP enables these IT controls.

SECTION 302: **CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS**

The CEO and CFO are required to personally sign each quarterly or annual report of financial information, certifying that the reports are materially correct.

- The signing officers are responsible for establishing and maintaining internal controls.

- The signing officers must design the internal controls so that material information is made known to the signing officers, especially during the period for which the financial reports are being prepared.

- The signing officers certify that they have evaluated the effectiveness of the company's internal controls as of a date within 90 days prior to the financial reports being issued.

- The signing officers present their conclusions in their report on the effectiveness of the company's internal controls as of that date.

IT Controls Requirements Summary

Complying with Section 302 means implementing an internal controls program that addresses the physical and digital risk points deemed to exist within the company's financial reporting operations. The PCAOB references an internal controls framework that companies should use when designing their internal controls program. This framework identifies five components of internal control: 1) control environment, 2) risk assessment, 3) control activities, 4) information, and 5) communication monitoring.

The widespread use of IT systems for financial information management makes IT controls critical for each of these components.

Application-level controls include preventive controls that prohibit certain changes in the system without additional authorization. Application controls also include monitoring. Monitoring occurs in the form of audit trails, which allow the re-creation of transaction history associated with key control processes. Monitoring controls also include triggers, alerts that are set to send notifications when certain situations occur within the system.

Access-level controls include security management specifying who can access and/or change what data, when, and within what timeframe.

Microsoft Dynamics GP Functionality

Microsoft Dynamics GP includes built-in functionality to enable application-level and access-level control to support compliance with section 302. This includes the ability to set up conditions within the system that require one or more authorized signers to electronically approve certain changes before they are able to proceed. System-change history associated with key control points can be automatically captured using the Microsoft Dynamics GP Audit Trails module. Audit trails can be turned on anywhere in the system, depending on the internal controls program of the company. Business alerts in Microsoft Dynamics GP can be set to trigger notifications by e-mail when certain conditions occur within the financial system. Audit trails and business alerts happen automatically and in the background, independent of user interactions. Microsoft Dynamics GP also includes access controls that support a company's internal controls program. Access controls include security within Microsoft Dynamics GP and are integrated with Microsoft network security. Microsoft Dynamics GP role-tailored security enables efficient management of segregation-of-duties policies. Other modules are available for managing the time of day and valid effectivity timeframe for user security in Microsoft Dynamics GP.

SECTION 404:   MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS

Company management is responsible for establishing and maintaining adequate internal controls and procedures, and a registered public accounting firm shall attest to, and report on, the assessment made by the management.

IT Controls Requirements Summary

Section 404 puts the responsibility on both management and external auditors to ensure that internal controls, including IT controls, exist. Therefore, auditors need to test the preventive and detective controls to obtain a high level of confidence that the controls exist and are functioning. Management must provide independent auditors with documentation and evidence of the functioning controls as well as documented results of tests that are performed.

Microsoft Dynamics GP Functionality

Using the electronic controls inherent in Microsoft Dynamics GP, managers are able to prove to auditors that the internal controls framework is in place and functioning. Auditors can see the controls activated online in the system, and they can recreate the electronic change history of key control points to prove that these points have operated effectively.

Because Microsoft Dynamics GP uses integrated financial reporting tools, managers can demonstrate that the company is not using manual interventions during the financial reporting process.

SECTION 409:   REAL-TIME ISSUER DISCLOSURE

Public companies must disclose changes in their financial condition or operations on a rapid and current basis to protect investors from delayed reporting of material events.

IT Controls Requirements Summary

Systems and processes must be in place and operating in such a way that they are ready to be used in a timely manner when material disclosures must be made.

The use of notifications based on condition alerts can indicate when conditions exist that would be considered material changes and enable for rapid identification and disclosure of material changes.

Microsoft Dynamics GP Functionality

Microsoft Dynamics GP helps ensure compliance with Section 409 by enabling businesses to capture financial information based on system-level transactions. Information can flow all the way through to financial reports without human intervention. For example, when users perform transactions related to customer orders, purchases, and vendor payments, information automatically flows through to the general ledger and to the corresponding financial reports. Since the reports are already in place, no additional compilation or manually-produced spreadsheets are required. Reports can be produced in real time whenever they are required and with the control needed to ensure that the information is not tampered with—as required by Section 302 and Section 404. It also enables the ability to disclose information rapidly to investors—in accordance with Section 409.

SECTION 802: **CRIMINAL PENALTIES FOR ALTERING DOCUMENTS**

Public companies and their public accounting firms are required to retain records, including electronic records, which impact the company's assets or performance. Fines and imprisonment are specified for those who knowingly and willfully violate this section with respect to (1) destruction, alteration, or falsification of records in federal investigations and bankruptcy and (2) destruction of corporate audit records. All audit information on key controls or the audit review itself must be maintained for a minimum of five years.

IT Controls Requirements Summary

Section 802 expects companies to respond to questions on the management of Sarbanes-Oxley-related content. This includes policy and standards on record retention, protection and destruction, storage as well as audit trails of key information that would enable an auditor to recreate the transaction history of processes where key controls exist.

Microsoft Dynamics GP Functionality

With automated business management systems like Microsoft Dynamics GP, most of the records that are relevant to Section 802 are electronically created and stored. In the case of actual transaction history associated with the application controls, these records tend to be in the form of structured data, stored within tables in a relational database. In the case of audit results, these records tend to be in the form of unstructured data, stored as separate files such as Microsoft® Office Excel® spreadsheets or Microsoft Office Word documents. Both types of records are needed to demonstrate compliance with Section 802.

Microsoft Dynamics GP deals primarily deals with structured data. To accommodate the requirements of Section 802, Microsoft Dynamics GP enables the ability to re-create the transaction history of any application controls, including tracking the time, date, user, change type, and before-change and after-change information. Information can be reassembled sequentially within Microsoft Dynamics GP to show the transaction history as it happened and when it happened. This audit information is stored in a separate Microsoft SQL Server™ database that runs parallel to the production SQL Server database for Microsoft Dynamics GP. The audit database can thus be controlled, secured, backed up, and retained according to policies and standards for record retention. For unstructured data, Microsoft Office Sharepoint® Server can serve as a repository to ensure that data is secured, controlled, backed up, and retained according to record retention policies.