The Keystone to Sarbanes-Oxley Compliance
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td><strong>Sarbanes-Oxley Keystone Components</strong></td>
<td>2</td>
</tr>
<tr>
<td>Accountability with Verifiable Segregation of Duties</td>
<td></td>
</tr>
<tr>
<td>Effective Mitigating Controls</td>
<td></td>
</tr>
<tr>
<td>Establishing Accountability</td>
<td>5</td>
</tr>
<tr>
<td>Corporate Structure and Business Process Relationships</td>
<td></td>
</tr>
<tr>
<td>Segregation of Duties Relationships</td>
<td></td>
</tr>
<tr>
<td>Business Process Profiles</td>
<td></td>
</tr>
<tr>
<td>User Roles</td>
<td></td>
</tr>
<tr>
<td>Establishing Change Control Processes</td>
<td>8</td>
</tr>
<tr>
<td>Final Suggestions</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

Sarbanes-Oxley compliance. Millions of pages of text are dedicated to Sarbanes-Oxley compliance. What is it? Why do we need it? How do we achieve it?

Yet, a survey conducted during a webcast hosted by Ernst & Young found that 38% of the participants cited "lack of guidance" as the biggest Sarbanes-Oxley 404 IT challenge\(^1\). Put another way by a Senior IT Auditor for a Fortune 300 Company, "the generality of the requirements, the lack of specifications" is the main SOX compliance challenge\(^2\).

So how do you tackle this challenge?

In its simplest form, Sarbanes-Oxley is intended to provide for a more accurate and transparent financial disclosure by public companies. Financial disclosures are produced from transactions maintained within the company’s systems and processes, building blocks of the organization, but requiring a keystone to maintain the integrity of the internal controls and structure.

The keystone to Sarbanes-Oxley compliance is to clearly define an application security structure that easily empowers individuals to complete their assigned responsibilities while providing accountability throughout the organization to minimize the risk of unauthorized activities. Glovia’s standard applications, including Security Manger and Audit Manger provide the tools for shaping the keystone to fit your specific business structure.

This white paper provides a non-technical, step-by-step process for developing the keystone for your company’s Sarbanes-Oxley section 404 requirements using Glovia.

---

\(^1\) Ernst & Young http://www.ey.com/global/Content.nsf/US/AABS - Assurance - Articles - TC Webcast 404 IT Issues

\(^2\) SOX insights from an IT auditor By Jeff Davis http://sarbanes-oxleyknowhow.bnet.com/sox_insights_from_an_IT_auditor.html
Sarbanes-Oxley Keystone Components

It is important to understand that section 404 of The Sarbanes-Oxley Act is broad, but not vague. It requires the maintenance of adequate internal controls and processes for financial reporting, and an annual assessment of the effectiveness of those internal controls. Now combine section 404 with section 409 which requires real time disclosure of material changes in the financial position or operations of the business and section 302 which requires both the Chief Executive Officer and Chief Financial Officer to individually certify the accuracy of the financial statements and the need for a comprehensive solution is necessary.

Organizations cannot efficiently achieve section 404 requirements for internal controls and annual assessments without a proactive approach with appropriate checks and balances. There are three main components to consider when establishing compliance with these Sarbanes-Oxley requirements: accountability with verifiable segregation of duties, effective mitigating controls and established change control processes.

These basic components apply throughout the organization, from the receiving dock to financial reporting to the board room, so incorporating them into your application’s implementation is critical. Using the following approach, you can provide clarity and communicate in plain English to employees, management and auditors a concise plan that will not only deliver SOX compliance through your application security framework, but establish a Sarbanes-Oxley compliant mentality for your entire organization.

Glovia’s Security Manager utilizes the application’s architecture to its fullest extent and provides the flexibility to establish responsibilities through an unlimited number of pre-defined “User Roles” that achieve segregation of duties requirements without sacrificing operational efficiencies. User Roles will prevent your IT staff, managers and employees from guessing which functionality they need to perform their responsibilities. Furthermore, predefined User Roles that meet the segregation of duties requirements should be implemented at different physical locations, ensuring consistency of operations throughout the organization.

The Audit Manager provides the on-line tools and reports necessary for establishing mitigating controls and monitoring change control processes. Identify your financially significant or high risk processes, activate the audit triggers and capture all activity down to the record level. Once this activity is captured it can be routed to the appropriate individual for notification and audit.

The end result is a practical way to consistently assign Glovia’s functionality to individual users and achieve Sarbanes-Oxley compliance, information guaranteed to minimize audit time and eliminate matters of interpretation from management.
Accountability with Verifiable Segregation of Duties

Accountability is achieved by assigning responsibilities to individuals in a two step process: assigning unique user identification for each individual accessing the application and ensuring verifiable segregation of duties for responsibilities assigned to individuals using User Roles.

Glovia provides two choices in establishing password protected access to the application based on the complexity of your business and your internal guidelines: a self-contained password protected three character user identification and synchronization to the UNIX operating system based eight character user identification processes. Both are SOX compliant as long as each user identification is unique to one individual and passwords are automatically changed on a predetermined basis.

From here, the framework for establishing adequate segregation of duties is a four step process:

- Establishing corporate structure and business process relationships
- Establishing segregation of duties relationships
- Establishing business process profiles
- Establishing User Roles

Effective Mitigating Controls

Despite best efforts, every organization encounter situations where it finds itself non-compliance with Sarbanes-Oxley due to segregation of duty conflicts. A small organization has only one individual responsible for the entire engineering process. A multi-shift division requires limited back up accessibility to prevent a shut down to operations if a problem is encountered. Wherever conflicting segregation of duty responsibilities exist, mitigating controls are required.

A mitigating control is simply a notification, requiring some type of action, to an authorized, independent third party when an individual exercises conflicting segregation of duty permissions. The notification can take on a number of forms: online notification, hardcopy report, email or workflow process using Glovia’s user portal, which provides a streamlined and efficient environment.

Regardless of the notification method, every situation requiring a mitigating control should be scheduled out so that the following information is available to management and auditors:

- Identification of the User Role, Business Process Profiles and functions with segregation of duty conflicts
- Identification of the independent third party with approval authority of segregation of duty conflicted activity
• Identify audit triggers activated in Glovia’s Audit Manager that capture conflicted activity
• Identify periodicity of notification to independent third party (immediate, nightly, weekly, other)
• Maintenance of documentation that the independent third party received the notification and acted upon it appropriately
• Periodicity of audit testing
• Records retention policy related to mitigating controls

A word of caution: unless you have good reason for doing so, mitigating controls should be established only at high risk functions and on the last possible process before a transaction becomes part of the permanent records of the company. Otherwise, you may incur unnecessary expenses resulting from potential excessive operating system overhead and redundant process reviews.
Establishing Accountability

Corporate Structure and Business Process Relationships
Defining your corporate structure and business process relationships is as unique as your fingerprint. You may be able to align each function with a department such as Accounts Payable, Receiving or Customer Service. Alternatively, you may decide to subcategorize within department for such activities as Planning and Scheduling. Or you may have multiple operating units with different consolidation requirements.

Glovia manages these requirements using Business Identification Number structure and Business Process relationships that are tailored to the complexity and resources of your specific operation. Regardless of the situation, your Business Identification Number and Business Process categories will be defined as a byproduct of the Major Business Processes document produced by the Glovia Implementation Team as standard practice in preparation of the application’s implementation.

Create a matrix of each Glovia function and assign it to one primary Business Process category.

Segregation of Duties Relationships
Basic segregation of duties ("SOD") categories include custody of assets, approval of transactions related to the assets, recording/reporting of data and control/verification of processes and transactions. However, additional SOD categories are advisable to take full advantage of Glovia’s flexibility to minimizing risk.

Non-IT functions should be assigned into one of seven basic SOD categories:

- "Menu" designates functions that provide access to menus, but not to menu functions. This is key to blocking users access to functionality that does not related to their responsibilities.
- "Inquiry" designates functions that provide access to review system data and obtain print screens so as to adequately perform their jobs, but not generate reports which could result in unsecured or improper transfer of proprietary information.
- "Reporting" designates functions that provide access to print, download or direct large volumes of data via predefined reports.
- "Process" designates functions that provide access to input, process or otherwise manipulate data and transactions within the application based on predefined standards.
- "Control" designates functions that allow for the establishment of predefined standards through the use of table files.
- "Custody" of assets designates the physical control of assets
- "Authorization" designates the approval of any controlled function.
IT functions, as gatekeepers for the integrity of the application, not the management of the business, should be assigned into one of seven different SOD categories:

- "Menu" designates functions that provide access to menus, but not to menu functions.
- "Inquiry" designates functions that provide access to review system data and obtain print screens so as to adequately perform their jobs, but not generate reports which could lead to unsecured and improper transfer of proprietary information.
- "Reporting" designates functions that provide access to print, download or direct large volumes of data via predefined reports.
- "System Administration" designates functions that provide application support, including purge and backup responsibilities.
- "Development" designates functions that support application implementation, programming, testing and validation.
- "Audit Administration" designates functions that establish audit framework and system change control parameters.
- "Security Administration" designates functions that establish security framework and user access.

**Business Process Profiles**

Business Process Profiles are used as the building blocks to define different User Roles and should be viewed simply as each major business process broken down into its seven segregation of duties categories. This is a mechanical process requiring no independent judgment, but it is a critical step in developing the framework.

The result of assigning Glovia’s functions to primary business process and segregation of duty categories should be two matrices, each listing Glovia’s functions down the left and the categories across the top. Now combine these two schedules into one matrix with the major business process categories as the primary category and the seven segregation of duties categories as secondary to each primary category. The result is that each function now belongs to one Business Process Profile.

The reasons for this classification is to group together all like functions for major business processes while clearly segregating functions that could allow someone to perpetuate and/or conceal errors or fraud.

An example of Business Process Profiles for the Purchasing process might be as follows:

- Purchasing - Menu: access purchasing menus and view which functions are accessible and not accessible
- Purchasing - Inquiry: review all purchasing and receiving data, but cannot process data
- Purchasing - Reporting: generate purchasing and receiving reports
- Purchasing - Process: create purchase orders and update vendor address file
• Purchasing - Control: maintain table files of approved purchase order numbers, approved vendors for purchasing, approved vendors for payment, buyers names and number
• Purchasing - Custody: physically receiving purchased assets
• Purchasing - Authorization: the approval of purchase orders

User Roles
Individuals are assigned “User Roles” to provide access to the application’s functions in specific pre-approved combinations. We define User Role by combining the Business Process Profiles that are minimally necessary for someone to perform their responsibilities. User Roles should be given simple names that relate to their functionality such as “Purchasing Agent”, “Purchasing Manager”, “Receiving” and likewise.

The benefits of standard User Roles are two fold. The non-technical user can request access to the application that will allow them to perform their responsibilities without the need to understand an ERP system’s complex structure. Standardization also ensures ease of administration and continuance of SOX compliance.

To define User Roles, create a matrix with User Roles listed down the left and Business Process Profiles across the top. Assign Business Process Profiles to User roles using the following rules:

• Non-IT User roles can contain any combination of Business Process Profiles for a specific business process as long as it does not contain more than one of the following segregation of duties categories: Process, Control, Custody, Authorization
• IT User Roles can contain any combination of Business Process Profiles for a specific business process as long as it does not contain more than one of the following segregation of duties categories: Security Administration, Audit Administration, System Administration, Development
• Users requiring access to information outside their primary business process should only receive inquiry or reporting access to the secondary business processes
• Any User Role failing to meet the above requirements require specific mitigating controls accountable to independent third parties

Deviations to the standard User Roles may be required. However, they should be severely scrutinized to understand the real basis for the request: Is the requested functionality absolutely required for an individual to complete their assigned responsibilities? If the requested functionality available through another menu under the same User Role? Should the responsibility be reassigned to another individual in accordance with the SOX compliant framework?

Regardless of the answer, deviations to standard User Roles should be the exception, not the norm. And all exceptions must be pre-approved by the designated compliance officer as part of the change control parameters described later.
Establishing Change Control Processes

A rigorous change control process is imperative to maintaining the integrity of the application security framework and passing an audit. Even the slightest deviation from the change control process can introduce doubt regarding the application security framework, requiring a complete review of the entire application and additional audit requirements.

The control process itself will reflect the structure and internal policies of the organization as a whole, but must include several key components:

a) All proposed changes to the application security framework must be analyzed in the context of the existing business process profiles, user profiles and mitigating controls.

b) All proposed changes to the application security framework must be approved by the designated SOX compliance officer(s) prior to implementation.

c) Authorized changes must be documented and centrally available.

d) Changes should be periodically audited to ensure compliance with authorization guidelines.

e) Independent audit should be provided the schedules supporting the critical points in a clear, concise format that expedited audit procedures without additional clarification.

Likewise, the same change control process should be applied to all financially significant and high risk processes. For example, an authorization table file exists to set the approval limits of individual with explicit rights to approve purchase orders, but changes to this table file should not be made unless they are made part of the approved change control process.

As for mitigating controls, change control processes should be established only for high risk functions and on the last possible process before a transaction becomes part of the permanent records of the company.
Final Suggestions

Following the outlined approach will result in a straight-forward SOX 404 compliant environment. You may also want to consider the following suggestions that will assist you in preparing the framework and ensure that you can explain your SOX 404 compliance utilizing your application’s security framework in a 30 minute presentation.

• Flowchart your change control process. Pictures are easier to follow than words.

• Build your matrices in Excel, Access or some other database compatible software. You can easily make revisions and upload them to the Security Manager throughout the Testing Phase, with final approved data uploaded to the Security Manager in the production environment.

• Differentiate the risk level of functions on your Business Process Profile matrix. If colors are available, highlight financially significant or high risk functions in red, processing functions in green, unimplemented functions in yellow and menu/inquiry/reporting functions in white. The color doesn’t matter, differentiating the risk does.

• Cross-reference all financially significant or high risk functions on the Business Process Profiles matrix to a separate schedule listing all internal controls or SOX 404 testing plans for that function.

• Ensure that every function on the Business Process Profiles matrix contains a description.

If you would like to know more about Glovia’s ability to establish a Sarbanes-Oxley compliant environment for your company, please visit www.glovia.com or call 800-223-3799.
International Headquarters
Glovia International, Inc.
2250 East Imperial Highway, Suite 200
El Segundo, CA 90245 U.S.A.
Toll Free: (800) 223-3799
Phone: (310) 563-7000
Fax: (310) 563-7300
www.glovia.com

EMEA
Glovia International B.V.
Gebouw “De Spoortoren”
Fellenoord 350
5611 ZJ Eindhoven
The Netherlands
Phone: +31 (0) 40-2655355
Fax: +31 (0) 40-2451444

Japan/Asia
Fujitsu Limited
17-25 Shin Kamata, 1 Chome
Ota Ku, Tokyo 144-8588 Japan
Phone: (01) 20-933-200
+81 (3) 6424-6122

United Kingdom
Glovia International, Ltd.
960 Capability Green Luton
Bedfordshire LU1 3PE
United Kingdom
Phone: +44 (0) 1582-635070
Fax: +44 (0) 1582-635270