Rapidly Reduce Segregation of Duty Violations in Oracle EBS R12 Responsibilities

Table of Contents

Introduction ............................................... 2
Access Controls ........................................... 2
Oracle Application Access Controls Governor ........................................... 2
Segregation of Duties Matrix ........................................... 3
Testing Roles Design ......................................... 4
Top Challenges ............................................ 5
Oracle EBS R12 Upgrade or Reimplementation ........................................... 5
Oracle Super Users .......................................... 5
Segregation of Duty Policies ........................................... 5
Complicated Security Model Increases SOD Risks ........................................... 6
Analysis of SOD Violation Incidents ........................................... 6
Key Factors Impacting SOD Violations ........................................... 6
SOD Controls Remediation – A permutation problem ........................................... 7
Controls Assessment Overview ........................................... 8
Assessment Approach ........................................... 8
ERP Assessment Tools .......................................... 9
Controls Selection ............................................. 11
Control Definitions and rules ........................................... 11
ERP Access Analytics .......................................... 12
Controls Implementation – Standard vs. Advanced Controls ........................................... 13
Role Design Techniques .......................................... 15
Create a Roles Catalog ........................................... 16
Create a Role from a Template ........................................... 17
Configure Role Entitlements ........................................... 17
Control Changes to Roles ........................................... 18
Deploy Role in Oracle EBS ........................................... 19
Roles Upgrade and Migration ........................................... 19
Case Study ...................................................... 21
Our Client ..................................................... 21
Challenges ..................................................... 21
Solution ....................................................... 21
Results ......................................................... 21
Conclusion ..................................................... 22
About FulcrumWay ........................................... 23
Introduction

As many organizations run their business on ERP Systems, such as Oracle E-Business Suite, PeopleSoft and J D Edwards, management must maintain effective ERP controls within the scope of the overall Governance, Risk and Compliance program. Business and IT managers should be familiar with how the ERP controls work and also have the right approach and tools to assess the control over enterprise applications that store, process and report business information. Well-designed ERP controls can improve business process effectiveness and accuracy while mitigating risks. For example, you can control the segregation of duty risks in a purchasing application to ensure that access to enter a supplier is separated from the access to make a payment to the same supplier. ERP controls can be of great value to the auditors in performing such an important task to ensure that the adequate controls exist. Like business controls, ERP controls should also be selected based on the risk assessed so as to reduce the impact of identified risks to acceptable levels.

In this paper, we will focus on Access Controls Management for Oracle EBS R12 Roles and Responsibility design. You will learn best practices to implement:

1. Responsibility templates from a catalog of pre-configured ERP roles.
2. Workflow to update, review as well as approve role design changes.
3. Roles management techniques to improve Security and SOD Control design.

Access Controls

Access Controls include controls over Segregation of Duties, User Provisioning and Access Verification process. For example, an employee may violate an access control if she/he has access to create supplier and approve payment. The Access controls audit includes assessment of the inherent design of application security roles that enable users to access the application functions as well as the risk of access granted to the users in each application function, menu, form, and module that support a business process.

Oracle Application Access Controls Governor

Oracle Application Access Controls Governor (AACG) is a segregation-of-duties control authoring and handling solution that works within and across ERP systems such as Oracle E-Business Suite and PeopleSoft to detect and prevents incidents of user access control violations. It can also be extended to monitor user access incidents in other off-the-shelf, custom and legacy applications including J D Edward, SAP, and Salesforce. Each AACG control specifies “entitlements” to a company’s business-management applications that should not be assigned simultaneously to individual users. AACG then finds users whose access grants violate access controls.
SEgregation of Duties Matrix

Segregation of Duties Control Objectives can be defined using an SOD Controls Matrix, which provides the framework to implement access controls consistently within and across business applications. The Access controls matrix-defined roles with access points across the rows and columns with confliction access levels identified in each cell. Application roles are design to provide user access to application data and functions based on the job descriptions and responsibilities. ACG tool tests application roles to ensure that the application security model complies with segregation of duty and access controls established by the organization. The security model of each application may vary, however, ACG provides consistent results based on the access points defined in the Access Controls Matrix. See example below:

In this example, the matrix provides a financial risk rating of access roles called “Responsibilities” in Oracle E-Business Suite that are assigned to a user. Each Responsibility should be designed to mitigate the access control violation risks. A responsibility design consists of menus, functions and options a user can access to process a transaction, change a setup or update a data object. The Oracle ACG software enables the IT auditor to test the security
model design that controls the use access based on the risk level identified in the access controls matrix. The auditor can view the access points within the E-Business Software and evaluate whether the design provides the level of control and granularity to selectively grant access as per the job requirements of all the users.

**TESTING ROLES DESIGN**

Once the role design is assessed, the auditor can also use the AACG software to verify whether all existing users have appropriate access as evidenced by their assigned Responsibilities and whether access to certain critical activities are allowed only to select, “privileged” employees duly authorized. AACG software also helps review the necessary access to administrator and “super user” rights and how such rights are assigned and controlled. Ideally no one in the IT group should have any access to the production data. All actions on the data by the super users should be logged and verified by the data owners regularly.
Top Challenges

Many organizations face challenges enforcing segregation of duty policies in Oracle E-Business Suite. Oracle seeded responsibilities have inherent SOD conflicts. For example GL Super User Responsibility enables the user to Enter Journal and Post Journal. This responsibility also enables the user to change ERP configurations such as key flexfields, GL Calendar, etc. EBS project implementation teams start with these “source” responsibilities to create “target” responsibilities that support business user functions. However, the Responsibility components such as Menus and Functions contain many access conflicts, which are not removed from the configuration.

**Oracle EBS R12 Upgrade or Reimplementation**

Oracle EBS upgrade patches introduce new SOD issues which further increases the risks of users gaining access to new function with potential conflicts. For example, R12 technical upgrade can add more than 10,000 new functions to more than 350 menus.

During EBS implementation or upgrade project, an effective approach is needed to Design and Test Oracle Security Model before deployment

**Oracle Super Users**

Oracle EBS “super users” Responsibilities are granted to some users to ensure that on-going system administration and maintenance. But the super users require effective compensating controls to maintain acceptable risk tolerance.

**Segregation of Duty Policies**

Selection of SOD policies that mitigate the risks in Oracle Responsibilities requires analysis of each EBS module that supports significant business process to determine the likelihood and impact of SOD control failures. This analysis requires comprehensive review of EBS configurations, master data changes, process workflow, and transactions.
**COMPLICATED SECURITY MODEL INCREASES SOD RISKS**

Oracle Security Model is based on one or more Responsibilities assigned to user. These responsibilities have many menus; each menu has many sub-menus and functions to access the Forms and Pages as shown below:

**Evaluate User Access**
- Test by User
- Test by Privilege

**Manage Segregation of Duties**
- Identify Incompatible Privileges
- Predefined & Extensible SOD Rule Sets

---

**ANALYSIS OF SOD VIOLATION INCIDENTS**

Access Controls testing tools can generate thousands of incidents and the process of closing these incidents can be time consuming.

Oracle Security model assessment generates many False Positives which need to be removed from SOD analysis.

**KEY FACTORS IMPACTING SOD VIOLATIONS**

Oracle EBS release (11i, R12) and Business Cycles such as Oracle to Cash, Procure to Pay, Record to Report, Hire to Retire, Design to Build, etc. enabled by Oracle modules determine the number SOD controls and incidents that violate these controls. For example, a typical Oracle EBS R12 customer has over 35,000 functions and 12,500 menus make up the access security model that needs to be assessed for SOD risks.

The number of SOD policies selected to control each business process and Oracle module determines the number of SOD violations. In our practice, we have seen a wide range of SOD controls in scope ranging from 25 to 250. The complexity of such controls also impacts the violations. For example, in Oracle AACG you can use the out-of-the-box entitlements or modify them as needed to reflect your use of business
applications, for example, customizations, personalizations and extensions to close the gaps between business requirements and ERP functions.

Number of Business Units and variation in Responsibilities across those business units impacts the SOD violations. Many organizations start with a single global template, but over time, business needs require variation of these standard responsibility configurations. Such variations cannot only increase the SOD violations, but also the time needed to correct the access control defects.

Advanced security implementations such as Role Based Access Controls (RBAC), Multi Org Access Controls (MOAC), Single-Sign-On, Identity Management, Multiple ERP system access, etc. require additional assessment of security model to ensure that SOD controls are effective.

The number of Users and Responsibilities assigned to those users impacts the number of violations. When user-responsibility assignments combinations have higher degree of variations, the SOD violations required more effort for analysis and remediation.

**SOD CONTROLS REMEDIATION – A PERMUTATION PROBLEM**

SOD violations require root cause analysis to create an effective remediation plan. However, this analysis can be a major challenge without advanced analytics because SOD violations represent the permutation in the Oracle security model. For example, Invoice Batches function used to create invoices is only of many “access points” that enables the users with access to AP_Navigate_GUI12 menu and AP_Invoices_Entry sub-menu as well as AP_Invoices_GUI12_G sub menu through multiple Oracle responsibilities including Payables Manager, US, Payables User, and Payables Supervisor as shown below:

```
Root Cause Analysis is required for remediation!

What if we exclude ‘Invoice Batches’ from AP_Invoices_Entry?
```

Copyright © FulcrumWay 2014
Controls Assessment Overview

Oracle EBS SOD controls assessment requires a structured approach to select the Oracle modules, SOD controls that provide coverage over the selected modules and data analysis tools to determine how the EBS control environment should be established using a system such as Oracle GRC Advanced Controls.

Assessment Approach

A risk based approach to Oracle EBS SOD controls assessment starts with the selection of risk impact and likelihood with each business process supported by Oracle modules. You can select the risks by business process and Oracle module from by searching through the ERP Risk Advisor available on FulcrumWay web site or contacting a FulcrumWay Risk Advisor to help you select the risk based on your business model. Once you select the risks, prepare an assessment checklist, which will include tasked required to analyze ERP system by risk type. There are seven major risk types that should be considered in complete assessment. These risk types include:

1. Access to ERP functions
2. Security Policies
3. Segregation of Duties
4. ERP system configurations
5. Master Data
6. Transactions
7. Effective Process Controls

Once you have prepared the checklist for assessment, you can create a ERP risk assessment “test” environment that can be recent clone of the production system, if that is not available, you can simply extract the security and configuration data from the production environment for testing. You can develop your own SQL scripts to execute the tests or you can download DataProbe from FulcrumWay web site, which includes pre-defined test scripts that cover all the major risk areas.

The results of the SQL test scripts or DataProbe output will provide you the evidence of ERP control effectiveness. For example, you can identify the Users and Responsibilities in Oracle EBS that violate the “Procure to Pay” SOD policy which requires a separation in access to Create Supplier and Approve Invoice functions. The results must be analyzed to eliminate false positives and identify any exceptions where internal controls mitigate the SOD risks. For example, if the AP Manager has access to Approve Invoice through the AP_VIEW_MENU, the violation may by false. If each Supplier creation or update is put on hold until a workflow approval is obtained by the VP of Procurement, then the SOD risk it mitigated.
After the analysis is completed, a findings report is prepared for review with application control owner. This is an important step to ensure that the managers closest to the business process can confirm the results and provide valuable feedback that may not be available in the ERP system or supporting documentation.

The findings report can serve as the business case for a remediation plan that may include changes to ERP security and configurations as well as implementation of advanced controls such as the Oracle GRC Advanced Controls software. At this stage, it is also important to create a project plan that ensures management sponsorship for adequate internal and external resources required for remediation and controls implementation.

The following diagram provides an overview of the assessment approach:

**ERP ASSESSMENT TOOLS**

The complexity of ERP systems such as Oracle E-Business Suite requires specialized SQL-scripts, or tools to evaluate the effectiveness of controls within each ERP module. For example, you can develop a script to extract the Oracle Users and Responsibilities using the following scripts:
You can also download a free utility program called FulcrumWay DataProbe™, which includes many of the scripts needed to start the risk assessment. FulcrumWay DataProbe™ is an easy to use ERP risk assessment tool that identifies ERP system vulnerabilities, unauthorized changes, as well as compliance to a wide range of regulatory mandates including Basel II, FISMA, FERC, HIPAA, NCR, OSHA, PCI DSS, and SOX.

ERP risk assessment tools and scripts are used by ERP system administrators, implementation consultants, internal auditors and external auditors in order to meet control objectives.

System Administrators assess application and database security. For example: complete list of users with access to Post Journal function in Oracle E-Business and users with access to employee personal identification information (PII) in Oracle HR tables. Payables Managers can confirm that ERP configuration for 3-way match in PeopleSoft 9.1 is configured to satisfy ERP SOX audit.

Systems Integrators test ERP system setups to ensure that ERP functions enable the customer business processes achieve expected business benefits and internal controls.

Internal Auditors evaluate ERP controls and sample transactions to assess operational risks such as Supplier Master Data Controls, Vendor Payment Controls, Revenue Recognition Controls and
Disclosure Controls. DataProbe is used for a wide range of audits including Recovery Audit, Fraud Audit, FCPA Audit, Supplier Audit, and Employee Expense Audit.

External auditors assert independent opinion over audited financial statements, in part, based on the ERP findings reports. The findings reports serve as evidence, which indicates operating effectiveness, significant deficiencies or material weakness of key controls over business processes enabled by ERP systems. Auditors can use this tool to follow a top-down risk based audit approach as directed by regulatory guidelines established by government agencies such as SEC and PCAOB in the United States.

**CONTROLS SELECTION**

The selection of the ERP controls for assessment should be based on the enterprise risks identified by management and the risk types included in the scope of the assessment. Oracle EBS R12 includes over 35,000 functions, which are configured using thousands to setup options to controls master data, and transactions. Therefore, a complete list of controls should be developed for an effective assessment. The following screen shot shows a listing of Oracle EBS objects from FulcrumWay Control Catalog that includes over 1,000 controls:

![Select SOD, Master Data, Setup, and Transaction Controls Risk Assessment](image)

**CONTROL DEFINITIONS AND RULES**

Each control selected for ERP Risk assessment must be defined based on the risk tolerance level determined by management. The risk tolerance varies by industry, business model and
management goals. For example, the security policy of a high-tech company requires may require user password changes every 90 days. A government agency may require Office of Foreign Assets Control (OFAC) evaluation of supplier master data available to AP Managers and Purchasing Supervisors. Oil Exploration and Production Company may choose to test duplicate payment control for AP Invoice over $10,000.

The following screen shows how you can configure the control rules based on your business risk tolerance:

**ERP Access Analytics**

The access control violation reports must contain information about all functions available to users through assigned EBS Responsibilities, which consist of menus, sub-menus and functions. Therefore, the reports can be large and complex. You can summarize this information using scorecards and graphs so managers can understand the results and make decision to remediate risks.
The following screen shows a set of Access Reports, ad-hoc analysis options, and a dashboard of Oracle EBS access violations by business unit in Oracle Application Express (Apex) page that is used to analyze the results:

**CONTROLS IMPLEMENTATION – STANDARD VS. ADVANCED CONTROLS**

Oracle EBS includes standard controls to control user access to ERP functions through Responsibilities. In addition you can use profile options, personalization, and data groups to further improve controls. However, the standard controls do not monitor or prevent access control policies. Oracle Application Access Controls Governor is part of the Oracle GRC Advanced Controls suite that enables you to continuously monitor segregation of duty controls and prevent assignment of Oracle EBS responsibilities to users on the Oracle security Form that could violation the SOD policy. The following diagram shows the modules included in Oracle GRC Advanced Controls:
Oracle Access controls implementation can simplify the SOD enforcement, simulation and remediation cycle by extracting and analyzing the EBS security configuration against the SOD policies selected by management for enforcement. The following screen shows an overview of Oracle AACG:
Role Design Techniques

Well-designed roles not only mitigate business risks but also improve user productivity. Seeded Oracle EBS Responsibilities provide an out-of-the-box catalog of “super user” responsibilities. However, these responsibilities require significant configuration effort to match organizations business roles and segregation of duty policies. You can use the seeded responsibilities as a source of templates to create target responsibilities that match your user role requirements. Each target responsibility can then be configured by creating custom menus that include or exclude functions to meet the entitlements for the target role. It is important to maintain change controls over the Oracle EBS security model to ensure that the process owners can review and approve Responsibilities based on business needs, organization structure and user roles. Once the roles and responsibilities are approved, you can deploy them in the Oracle EBS system for testing. You can also use these techniques to migrate Oracle EBS Responsibilities from one version to the next during an upgrade.
CREATE A ROLES CATALOG

You can accelerate the Oracle EBS responsibility configuration tasks by creating a global catalog of all approved roles that are required by the business. We maintain a list of widely used Oracle EBS Responsibilities in a Roles Catalog that is available in the FulcrumWay controls cloud. For example, for Oracle General Ledger responsibilities such as Manager, Supervisor, Clerk, Inquiry, Business Setup and IT Setup are included in the roles catalog. You can use these responsibilities as templates and create your company specific responsibilities that have segregation of duty controls pre-configured by design as shown below:
CREATE A ROLE FROM A TEMPLATE

Once you select a template as a source, you can create a target role for a selected Oracle EBS environment and application. You can also add the comments for role reviews and approvers. If you need to remediate and SOD risks, you can also see any violations of your SOD policies in summary to detail before you start changing the role configuration:

CONFIGURE ROLE ENTITLEMENTS

Each role can be modified by selecting to de-selecting business activities or “entitlements” within the Oracle security model hierarchy and the tool automatically reconfigures the Oracle EBS Responsibility to save you time and reduce configuration errors. You can also select concurrent requests available to the user through the role.
Once you complete the role configuration, you can submit the role to pre-assigned reviewers and approvers. In addition, the Oracle EBS security administrator can also be notified to load the Oracle Responsibility LD1 file using FNDLOAD program. The following screen shot shows the Role approval workflow options available with the roles manager:
DEPLOY ROLE IN ORACLE EBS

You can deploy the Responsibilities in Oracle EBS environment for testing by downloading the ldt files from the Roles Manager and upload these files using the FNDLOAD program as shown below:

ROLE UPGRADE AND MIGRATION

Oracle EBS Upgrades introduce new functions in the Oracle security model – whether you choose technical upgrade by patching the old environment or a re-implementation starting with vanilla install. Upgrade projects require a rigorous and time consuming analysis of old vs new Oracle Responsibility comparisons to ensure that loss of functionality can be minimized while new functions are assigned to the users. Also, it is important to ensure that the new functionality does not increase the Segregation of Duty and sensitive data access risks above the risk tolerance levels. You can streamline the role upgrade and migration activities by creating a Responsibility Comparison Report. Once you do a side-by-side comparison of old vs new responsibility, you can choose the menus and functions for the target responsibility. The following example shows a comparison of HK General Ledger Lead Responsibility in 11i against the General Ledger R12 Responsibility:
<table>
<thead>
<tr>
<th>Source Environment</th>
<th>Source Responsibility Name</th>
<th>Source Parts</th>
<th>Source Function Name</th>
<th>Source Available</th>
<th>Target Environment</th>
<th>Target Responsibility Name</th>
<th>Target Parts</th>
<th>Target Function Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>RT 11A.50</td>
<td>General Ledger Lead</td>
<td>RMD4H45</td>
<td>Multi-Sell</td>
<td>Yes</td>
<td>RT 70G2E.12</td>
<td>General Ledger Super User</td>
<td>RMD4H45</td>
<td>Multi-Sell</td>
<td></td>
</tr>
<tr>
<td>RT 11A.50</td>
<td>General Ledger Lead</td>
<td>RMD4H45</td>
<td>Column Sell</td>
<td>Yes</td>
<td>RT 70G2E.12</td>
<td>General Ledger Super User</td>
<td>RMD4H45</td>
<td>Column Sell</td>
<td></td>
</tr>
<tr>
<td>RT 11A.50</td>
<td>General Ledger Lead</td>
<td>RMD4H45</td>
<td>Define Mesh Order</td>
<td>Yes</td>
<td>RT 70G2E.12</td>
<td>General Ledger Super User</td>
<td>RMD4H45</td>
<td>Define Mesh Order</td>
<td></td>
</tr>
<tr>
<td>RT 11A.50</td>
<td>General Ledger Lead</td>
<td>RMD4H45</td>
<td>Parcels Screen</td>
<td>Yes</td>
<td>RT 70G2E.12</td>
<td>General Ledger Super User</td>
<td>RMD4H45</td>
<td>Parcels Screen</td>
<td></td>
</tr>
<tr>
<td>RT 11A.50</td>
<td>General Ledger Lead</td>
<td>RMD4H45</td>
<td>Parcels Screen</td>
<td>Yes</td>
<td>RT 70G2E.12</td>
<td>General Ledger Super User</td>
<td>RMD4H45</td>
<td>Parcels Screen</td>
<td></td>
</tr>
<tr>
<td>RT 11A.50</td>
<td>General Ledger Lead</td>
<td>RMD4H45</td>
<td>Parcels Screen</td>
<td>Yes</td>
<td>RT 70G2E.12</td>
<td>General Ledger Super User</td>
<td>RMD4H45</td>
<td>Parcels Screen</td>
<td></td>
</tr>
</tbody>
</table>
Case Study

OUR CLIENT

- Leader in the car and equipment rental businesses worldwide
- Providing quality car rental service for over 90 years
- Over 30,000 employees

CHALLENGES

- Replace multiple legacy systems with one ERP solution
- Improved Segregation of Duty controls within mission critical applications
- Maintain consistent ERP system access roles across the subsidiaries leveraging the shared services model
- Increase external auditor’s reliance on ERP Access Controls Monitoring

SOLUTION

- GRC DataProbe™
- ERP Controls Catalog
- ERP Roles Monitor

RESULTS

- Reduce ERP Role design, build, testing and implementation time by 80% resulting in over $200,000 cost savings during ERP system implementation and global rollout.
- Created over 100 Segregation of Duty compliant Roles by business segment with two weeks from FulcrumWay Role Templates within the controls catalog.
- Lowered ERP Total Cost of Ownership by reducing SoD remediation time and costs by ensuring that all users are assigned only the pre-approved Roles
- Improve SoD and Access Controls testing time by providing auditors the access log reports showing all Update, Review and Approve Role design changes.
- Accelerated ERP testing and deploying time by identifying SOD conflicts before the Roles are assigned to Users.
Conclusion

In this white paper you learned to design Roles and Oracle Responsibilities that rapidly reduce the segregation of duties risk in Oracle E-Business Suite.

Segregation of Duty controls are a significant component of control environment of any organization that operates its business on an ERP platform such as Oracle E-Business Suite. Oracle Application Access Controls Governor (AACG) is available as part of the Oracle GRC Advanced Controls suite to help Oracle customers enforce SOD policies in Oracle EBS. You can use a SOD Matrix to select the conflicting business activities and establish SOD polices in Oracle AACG based on your business model and tolerance for risk.

There are a number of challenges in addressing the segregation of duty controls in Oracle E-Business Suite because of a complex hierarchal security model, control design defects in the super-user responsibilities “seeded” within EBS, and configuration of your EBS applications. Analysis of SOD violations can also be complex and time consuming due to the large number of incidents and false-positives generated by the SOD controls testing tools. The number of business units, variation of responsibilities across those business units, advanced security options, customizations and number of SOD policies also impact the effort required to remediate SOD risks.

You can estimate the effort to implement ERP controls and develop a business case for Oracle GRC Advanced Controls by assessing the risks in Oracle EBS modules in scope for your organization. The control definitions should include business description of the risk and the corresponding EBS technical configuration that is mapped to the risk. You can create the risk assessment reports using SQL scripts or audit tools such as Dataprobe, which is freely available for download from FulcrumWay web site.

Effective role design techniques can help you rapidly reduce SOD and other access risks by embedding the controls in the Oracle EBS Responsibly design. We recommend use a roles catalog that is reviewed and approved by business process owners to ensure that the Oracle EBS Responsibilities meet business requirements and risk tolerance levels of your organizations. You can use this catalog as template to configure additional Oracle EBS responsibilities by enabling or disabling the menus and functions within the target responsibility. Once the role design is reviewed and approved, the EBS system administrator can use the LDT file generated by the Roles Manager to upload the Responsibility configuration file into Oracle EBS using the FNDLOAD program. You can also use this approach to migrate Oracle EBS Responsibilities across EBS instances and Oracle EBS versions during upgrades.
About FulcrumWay

Fulcrum Information Technology, Inc. d/b/a FulcrumWay is US C Corporation registered in the State of Delaware and headquartered in Dallas, Texas. FulcrumWay is a privately held corporation, serving clients in North America with a regional presence in California, New York, and Texas, as well as clients in Latin America, Europe, Middle East, Africa, and Asia with international presence through a partner network and technology solution center in India.

FulcrumWay is a leading provider of Enterprise Risk Management (ERM) solutions that help organizations rapidly assess enterprise risks reliably execute business processes and easily monitor internal controls to gain strategic advantage. FulcrumWay’s deep ERM domain expertise, proven solutions delivery methodology and integrated software services platform enable organizations to leverage information technology investment and turn governance, risk and compliance challenges into better business performance. FulcrumWay is a privately held Delaware corporation, serving clients in North America with a regional presence in California, New York, and Texas, as well as clients in South America, Europe, Middle East, Africa, and Asia through our partner network and technology solution center in India.

We provide Rapid, Reliable and Easy Access to Business Risk & Compliance Management, Continuous Controls Monitoring, Enterprise Risk Management, ERM Integration, IT Governance and Risk & Compliance Automation through:

**Expertise:** Since 2003, we have engaged over 100 Fortune-500 and Middle Market companies across all major industries in key risk and compliance areas. Our highly experienced and qualified professional advisors guide organizations based on their deep knowledge of governance, risk and compliance best practices, templates and tools. We work side by side with Audit, Compliance, Risk, Finance, and IT Managers to streamline and improve ERM processes. FulcrumWay professionals deliver management consulting, enterprise software selection, implementation, training and support services.

**Packaged Solutions:** We are the leading provider of Risk Management, Compliance Automation and Internal Control Solutions for organizations running ERP Systems. We help organizations implement packaged solutions that are designed to be reliable, flexible, scalable and adaptable to meet key business objectives. Organizations can select the right combination of on-site and remote resources to achieve the desired level of service and cost objectives. Our proven solution delivery methodology brings together powerful combination project management skills, extensive expertise in ERM systems implementation, pre-defined deliverables, process flows, world-class cloud services and around the clock infrastructure support that helps organizations achieve faster investment payback and mitigate solution deployment risks.
**Software Services:** We are the leader in financial, operational and IT risk assessment, as well as business process assurance and internal controls monitoring software services that are easily accessible to organizations immediately on-demand over a reliable, secure internet connection using a web browser. FulcrumWay Software Services are designed to help organizations mitigate enterprise risk, enhance the quality of financial reporting and improve visibility into enterprise performance metrics. The software services are fully integrated to "plug" into an organization’s existing IT systems without requiring costly hardware or software installation. Organizations access our software services to quickly and comprehensively address key risk and compliance challenges such as how best to correct segregation of duty issues, monitor access, manage system configuration controls, analyze suspicious transactions, assess internal controls, streamline financial reporting controls and share ERM information across the enterprise.