MANAGING SECURITY AND SEGREGATION OF DUTIES IN DYNAMICS

GP, AX and 365

March, 2019
The Presenters

**Kari Sklenka-Gordon**
Director, National Leader of ERP, Analytics and Continuity Risk
- 17+ years experience in GRC transformation
- 11+ years in public accounting in both internal and external auditing
- Executed 40+ SOD assessments covering more than 30 types of large scale ERPs, application and custom developed applications
- Developed RSM SOD methodology & approach
- Assisted with over 20 GRC implementations

**Matt Wilson**
Director, Dynamics GP Practice Leader RSM Southeast
- 22+ years experience with Dynamics GP implementation and support
- Wide variety of industry experience including Healthcare, Professional Services, and Nonprofit
- Certified Public Accountant

**Kevin Giardini**
Manager, Dynamics 365 Managed Application Services
- 8+ years of Dynamics AX 4.0, 2009, 2012, and D365 F&O consulting experience
- Microsoft certified in D365 Financials and AX development
- Supported and assisted with 40+ client implementations
- AXUG Summit and AXUG Focus presenter
Agenda

• RSM’s Dynamics & GRC technology capabilities
• What are SODs?
• Dynamics Security Hierarchy & Security Management leading practices:
  ▪ GP
  ▪ AX
  ▪ 365
  ▪ RSMs SOD Methodology
  ▪ Fastpath
RSM’s Dynamics Capabilities

- Implementer of all Dynamics applications
  - Inner Circle Partner for Microsoft
  - Presidents Club Partner for Microsoft
  - Gold Certified Partner for Microsoft
- FastPath (GRC technology) Reseller
- Dynamics Segregation of Duties & Automated Application Controls Design & Assessments
RSM’s Proven Experience

RSM has performed over 60 SOD assessments covering all major ERPs as well as many unique industry-specific, highly customized, and home grown applications.

RSM has experience with all major ERP GRC controls monitoring tools, and is a reseller and implementer of many of them.

RSM Partnerships
Today’s webcast will cover

• Dynamics GP
• Dynamics AX
• Dynamics 365 Finance & Operations (AX)
• Dynamics SL
• Dynamics 365 Business Central (NAV)
WHAT ARE SODS?
Key Sensitive Functions & Segregation of Duties

- **Key Sensitive Functions** are tasks, manual or automated, which are critical to support the business, financials, or regulatory requirements.

- **Segregation of Duties (SoDs)** separate key sensitive functions, where if combined can result in fraud, misuse, or errors. When in place, SoDs can detect or prevent errors or fraud.
# Common Functional SOD Activities

<table>
<thead>
<tr>
<th>Activity 1</th>
<th>Activity 2</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate</td>
<td>Approve</td>
<td>Initiate a purchase order vs. approve a purchase order</td>
</tr>
<tr>
<td>Create</td>
<td>Post</td>
<td>Create a journal entry vs. post a journal entry</td>
</tr>
<tr>
<td>Transact</td>
<td>Reconcile</td>
<td>Enter information related to financials vs. responsibility for reconciling financial data</td>
</tr>
<tr>
<td>Develop</td>
<td>Promote</td>
<td>Develop code or system changes vs. promote (approve) changes to production.</td>
</tr>
<tr>
<td>Maintain Master Data</td>
<td>Transact</td>
<td>Create new customer master data vs. Create sales order.</td>
</tr>
<tr>
<td>Business Actions</td>
<td>IT Actions</td>
<td>Manage business operational activities in an ERP vs. manage IT support operations of the ERP</td>
</tr>
</tbody>
</table>
SODs are more than just update access

- You may have GDPR or PII regulatory requirements of which you may need to separate even display access
- Fraud can also occur when individuals have display access combined with update access
AICPA Guidance:

SOD is a basic building block of sustainable risk management and internal controls for a business.

The principle of SOD is based on *shared responsibilities of a key process* that disperses the critical functions of that process to more than one person or department.

Without this separation in key processes, fraud and error risks are far less manageable.

Source: https://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Auditing/InternalControl/Pages/value-strategy-through-segregation-of-duties.aspx
Summary value of Segregation of Duties

Segregation of duties value:

• AICPA
• SOX
• FDA
• Fraud
• PII
• GDPR
DYNAMICS GP SECURITY HIERARCHY
GP Security Hierarchy Model Overview

20,000

Activities/Security Objects

Tasks

Roles

Users
GP functional view of security

Role

Task

Security Objects
GP Security – Ways to Alter/Change or Conceal

• Ability to change master record information after activity is posted

• Changing out of the box or custom security roles and task
Level setting GP SOD exception types

USER ID A ➔ Role AP
USER ID A ➔ Role AR

USER ID A ➔ Role AP with AR
Leading Practice GP security management

• GP Roles are NOT SOD-compliant out of the box
• To be SOD-compliant, custom roles must be created for your organization
• GP allows security to be based on windows, reports, and posting permissions
  – For example, if you want to prevent someone from add/modifying vendors, remove the Vendor Maintenance window.
  – If you still want the user to be able to view vendors, give them the Vendor Inquiry window which contains the same fields as Vendor Maintenance but they’re all dimmed
• GP also allows field-level security but very few clients adopt this
Leading Practice GP security management: Automated Mitigating Control Options

• GP 2013 and above includes workflow approvals for Payables, Purchase Orders, GL Journals, and Vendor Maintenance

• GP includes batch approval functionality that can be used when a complex workflow is not required.
DYNAMICS AX 2009 SECURITY HIERARCHY
Overview of User Group Based Security (AX 2009)

- User Group
  - Security Key
    - Securable Objects
      - User Interface Elements (Forms)
      - Tables and Fields
      - Reports
Leading Practice AX 2009 security management

• No out of box SOD exists
• Limit number of user groups
• Limit the number of security keys
• Avoid field level security
• Workflow and other mitigating factors should be considered when assigning security
DYNAMICS AX 2012 & 365 SECURITY HIERARCHY
Overview of Role Based Security AX 2012 & D365

- Roles
- Duties
- Privileges

Securable Objects

- User Interface Elements (Forms)
- Tables and Fields
- SSRS Reports
- Service Operations
AX 2012 & D365 Security Hierarchy

Diagram showing the security hierarchy with roles, duties, privileges, and permissions.
Verify whether user role assignments comply with new rules for segregation of duties

View and resolve conflicting user role assignments

Verify whether existing roles comply with new rules for segregation of duties
Leading Practice AX 2012 & D365 security management

• Each out of box role lines up with SOD
• Conflicts occur when multiple roles are assigned
• SOD rules are not defined
• If modification to security need to be made, duplicate base roles for development
• Workflow and other mitigating factors should be considered when assigning security
RSM’S SOD ASSESSMENT APPROACH
RSM’s comprehensive SOD Assessment Methodology

RSM’s SOD Assessment Methodology/Approach

Phase I: SOD Modeling
Phase II: SOD Technical Security Modeling
Phase III: SOD Analysis & Remediation Approach
Phase IV: SOD Elimination
Phase V: Rerun SOD Analysis; Mitigating Controls Identification
Phase VI: SOD Operational Process Improvement
RSM SOD Modeling Methodology

• Identify key business activities through workshops using RSM’s leading practice sensitive activity accelerator which contains:
  • 129 Business Process Activities
  • 24 IT Process Activities

  – Resulting in leading practice SOD combinations with risk ratings
    • 224 Business Process SOD combinations
    • 16 IT Process SOD combinations
    • Including a cross-business transaction user vs. IT support user SOD check
Flexible as we can add additional business process activities; new SOD combinations if needed.

**RSM Business Process Activities**

<table>
<thead>
<tr>
<th>Business Process</th>
<th>New Business Process Activity</th>
<th>Leading Practice Risk Rating</th>
<th>Unique Business Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order to Cash</td>
<td>2.27 Med</td>
<td>Maintain or authorize accounts receivable allowance adjustments</td>
<td></td>
</tr>
<tr>
<td>Order to Cash</td>
<td>2.28 High</td>
<td>Authorize write-offs of delinquent accounts</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.01 High</td>
<td>Maintain purchasing system configuration</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.02 High</td>
<td>Create or Change Vendor Master Records</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.03 High</td>
<td>Approve Vendor Master Data Changes</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.04 Med</td>
<td>Create or Change Purchase Requisition</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.05 Med</td>
<td>Approve or Release Purchase Requisitions</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.06 High</td>
<td>Create or Change Purchase Order</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.07 High</td>
<td>Approve Purchase Order</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.08 High</td>
<td>Process Vendor Invoice (Enter vendor invoice to system to match to goods receipt or services rendered)</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.09 High</td>
<td>Approve Vendor Invoice (for non PO purchases)</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.10 Med</td>
<td>Create vendor debit memo (or AP voucher)</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.11 High</td>
<td>Approve vendor debit memo (or AP voucher)</td>
<td></td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>1.12 High</td>
<td>Processing Payment to Vendor (create payment to vendor, create check or wire or EFT)</td>
<td></td>
</tr>
</tbody>
</table>

**RSM Business Process Segregation of Duties Methodology**

<table>
<thead>
<tr>
<th>Risk (H/M/L)</th>
<th>New Risk #</th>
<th>Business Process</th>
<th>Risk/What could go wrong</th>
<th>Business Activity 1</th>
<th>Perform or Approve (P/A)</th>
<th>Business Activity 2</th>
<th>Perform or Approve (P/A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>1.03</td>
<td>Purchase to Pay</td>
<td>An individual could create a fictitious purchase order and direct disbursements for these purchase orders</td>
<td>Create or Change Purchase Order</td>
<td>P Processing Payment to Vendor (create payment to vendor, create check or wire or EFT)</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>1.04</td>
<td>Purchase to Pay</td>
<td>An individual could create a fictitious purchase order and fraudulently receive goods against the vendor</td>
<td>Create or Change Purchase Order</td>
<td>P Receives goods into Warehouse/Plant (Process Goods Receipt)</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>1.05</td>
<td>Purchase to Pay</td>
<td>One individual could approve, enter purchase order bypassing dual signing</td>
<td>Create or Change Purchase Order</td>
<td>P Approve Purchase Order</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>1.06</td>
<td>Purchase to Pay</td>
<td>An individual could create a purchase requisition for unauthorized goods and approve the unauthorized purchase requisition</td>
<td>Create or Change Purchase Requisition</td>
<td>P Approve or Release Purchase Requisitions</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>1.07</td>
<td>Purchase to Pay</td>
<td>An individual could create fictitious vendor or alter vendor name/address information</td>
<td>Create or Change Vendor Master Records</td>
<td>P Approve Purchase Order</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>1.08</td>
<td>Purchase to Pay</td>
<td>An individual could create fictitious purchase</td>
<td>Create or Change Vendor Master Records</td>
<td>P Approve Purchase Order</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>1.09</td>
<td>Purchase to Pay</td>
<td>An individual could create fictitious vendor or alter vendor name/address information</td>
<td>Create or Change Vendor Master Records</td>
<td>P Process Vendor Invoice (Enter vendor invoice to system to match to goods receipt or services rendered)</td>
<td>P</td>
<td></td>
</tr>
</tbody>
</table>

**Business Process**

<table>
<thead>
<tr>
<th>Business Process</th>
<th>Sensitive Actions</th>
<th>SODs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record to Report/ Close (includes Cost Accounting, Treasury, Tax)</td>
<td>33 49</td>
<td></td>
</tr>
<tr>
<td>Fixed Assets</td>
<td>18 29</td>
<td></td>
</tr>
<tr>
<td>Order to Cash</td>
<td>28 61</td>
<td></td>
</tr>
<tr>
<td>Purpose to Pay</td>
<td>16 45</td>
<td></td>
</tr>
<tr>
<td>Hire to Retire</td>
<td>11 12</td>
<td></td>
</tr>
<tr>
<td>Inventory</td>
<td>23 28</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>129 224</strong></td>
<td></td>
</tr>
</tbody>
</table>
SOD Technical Security Modeling for Dynamics

• RSM will review all security objects in your Dynamics environment, including customized objects, and map them to your customized SOD model out of phase 1.
• RSM will provide a template which can be uploaded into your SOD tool.

What if you don’t have a GRC technology?

You can lease Fastpath through RSM, and we can upload it into our tool.
Why is technical SOD modeling important?

• Customize to meet “your” needs:
  – Key business activities
  – Risk
  – Customizations to Dynamics
Analysis/ Remediation

• After the analysis is performed, RSM can assist with remediation determination as well as assisting with the actual remediation for Dynamics

• Approach is through work-shops

Can’t remediate the SOD through security? Mitigate!

RSM has a catalog of over 400 business controls that can be selected from for mitigation
SOD Governance

• Are you managing security in a leading practice way for your Dynamics systems?

• Is your provisioning process the most ideal for incorporating segregation of duties assessments into each user/role assignment?

• Are you utilizing technology or analytics where possible to prevent and detect SODs?
Is a GRC technology really that helpful?

• GRC technology can detect potential SOD conflicts before the conflicts are assigned in production

• GRC technology can quickly assess cross SOD conflicts faster than a manual review

• Mitigating controls can be stored in a GRC technology
FASTPATH
What is a GRC technology?

- Governance, Risk & Compliance Technology
  - Segregation of Duties
  - Access Certifications
  - Access Reviews
  - Change Management Tracking
  - User Provisioning
  - Single Sign-on
Fastpath GRC Products for Dynamics

Fastpath ensures our customers can confidently answer these three critical questions:

Who has access to their systems?
What did they do with that access?
Where are they vulnerable?

Assure
Segregation of Duties and Security Access Reviews

Identity Manager
Compliant User and Emergency Access Provisioning

Audit Trail
Critical Data Change Tracking

RSM is both a certified reseller and implementer of Fastpath, as well as a user of it for our clients.

©2019 RSM US LLP. All Rights Reserved.
Fastpath technology options

• Purchase your own Fastpath technology
or
• You can “lease” Fastpath at a discounted fee through RSM, as RSM provides the services to update the rules, or to run the analysis.

RSM can assist in coordinating a demo of Fastpath that works for your Dynamics or ERP landscape.
SUMMARY
Summary of what you heard today

- Segregation of duties in your ERP is good practice to have, and should be performed regardless if you are highly regulated or not.
- Dynamics security is complex with lots of configuration options including custom configuration.
- Dynamics has lots of automated migrating controls.
- Segregation of duties assessment is best done during an implementation.
- Once you have a “clean” Dynamics environment free of SOD exceptions, you should implement governance procedures around user /role provisioning which we highly recommend it includes a GRC technology, like FastPath
- FastPath can either be sold or leased through RSM