Building a Sound Security and Compliance Environment for Dynamics AX and Dynamics 365 for Finance and Operations

Presented by:

Frank Vukovits
Director – Strategic Partnerships, Fastpath

Aaron Hamilton
Senior Systems Accountant, Texas Roadhouse

D365UG | AXUG

Your Co-Presenter

Frank Vukovits

FASTPATH

D365UG | AXUG

Director of Strategic Partnerships at Fastpath

Original co-founder of AXUG

Experience goes back to Axapta 3.0 SP1 (2003)

Certified Internal Auditor

Certified Information Systems Auditor

Twitter: @Fvukovits

Your Co-Presenter

Aaron Hamilton

Senior Systems Accountant for Texas Roadhouse

16 years at Texas Roadhouse, started as a bus boy

Manages Security and Maintenance within Dynamics AX

Texas Roadhouse Went Live in 2016 with 150 Users

Session Objectives

Upon completion of this session, participants should be able to:

1. Understand the six different pillars of controls monitoring, as defined by Gartner.
2. Understand how in Dynamics AX and Dynamics 365 for Finance and Operations, controls monitoring can be accomplished, both manually and in an automated function (sometimes).
3. Understand why controls are important and help minimize risk, regardless of company size, public, or private.

Session Agenda – Six Pillars of Controls Monitoring

Risk analysis

Access certification

Role management

Compliant user provisioning

Emergency access management

Continuous monitoring

These six pillars are the industry standard from Gartner© and require the deployment of a combination of detective, preventative, and reactive controls to be effective within Dynamics AX/D365FO.

Gartner's Review on Controls Monitoring

"Analyzing risks and monitoring controls within business applications including ERP and other financial systems is a challenge for most organizations. Compliance and IAM leaders should consider automated solutions for improving control over SOD risks for key business systems."

Source: Gartner© G00272271, April 28, 2015

Six Pillars of Controls Monitoring

- Risk analysis
- Access certification
- Role management
- Compliant user provisioning
- Emergency access management
- Continuous monitoring

Risk Analysis

Detects SOD conflicts, sensitive access, and potential policy violations for existing users through the use of business-oriented rules that are mapped to specific applications' authorization models.

This is a DETECTIVE control

Risk Analysis

- What are your Business Rules?
  - Review business process maps from implementation or upgrade projects
  - Identify users in business process functions
    - Determine what users need access to
    - Determine what type of access users require in these areas
- Engage Appropriate Parties
  - Business Process Owners
  - IT
  - Partner
  - Internal Audit (if applicable)
  - Executives

Risk Analysis

- This Exercise Should be a part of a Larger Risk Assessment Exercise
  - Critical risks are graded high, medium, or low
  - Let the system do the work - that's the mapping piece of the exercise when it comes to security provisioning
  - Directly Feeds the Next Pillar - Access Certifications

In the AX World, very often provisioning of security is an exercise performed during the implementation or upgrade project and not tied to any other company wide activities, such as an annual risk assessment.

Access Certifications

Automates the periodic recertification of users' access by supervisors, role owners, or process owners.

This is a DETECTIVE control

Access Certifications

- Identify high risk business processes
- Map the processes to Dynamics AX and D365FO security
- Identify administrator access
- Choose a reviewer and a schedule
  - Business process owners vs. security admins
- Provide evidence of the review

In the AX World, limited security reviews are often performed, because there is not good data to review, assignments are not documented originally, or reviews are too time-consuming.

Role Management

Provides mechanisms for role design as a means to reduce SOD conflicts and improve administration efficiency. This usually includes a mechanism for transporting new or updated role definitions into appropriate application environments.

This is a PREVENTIVE control

Role Management

- Focus on security before you Go Live
  - Initial implementation
  - Upgrade
- Minimize vs. eliminate risk
- Role-based implementation plan

In the AX World, security is often an afterthought of the implementation or upgrade. Provisioning security can be long, and can lead to less than thorough assignments, or worse, securing less, due to time required to provision security for all users correctly.

Compliant User Provisioning

Automates account provisioning and enforces preventive controls through access requests, policy analysis, selection of mitigation controls (if necessary), and workflows for approvals and fulfillment.

This is a PREVENTIVE control

Compliant User Provisioning

- Access Should Be
  - Permanent or Temporary
  - Documented
  - Reviewed
- Appropriate SOD Around Granting of Access

In the AX World, often the requesting and subsequent administration of security is burdensome. The process takes a long time, is not easy to perform, and non-IT users find it especially difficult to understand.

Emergency Access Assignment

Provides users with temporary access to elevated or conflicting privileges and monitors usage of the access.

This is a PREVENTIVE control

Emergency Access Assignment

- Access Should Be
  - Temporary
  - Documented
  - Reviewed
- Auditors Always Ask About This

In the AX World, often users are given System Administrator role access to help troubleshoot a problem, and that access is never revoked.

Continuous Monitoring

Monitors transaction activities in ERP and other enterprise applications to detect SOD failures and responds accordingly.

This is a DETECTIVE control

Continuous Monitoring

- Setup/Performance
  - Take a risk-based approach
  - If you aren't going to report on it, don't track it
- Reporting
  - Who? What? When?
- Data maintenance
  - Retention policy
- You can add transaction monitoring as a detective control - This takes you outside of SOD review, but that is okay

In the AX World, monitoring of security often does not occur because of how difficult such an exercise is to perform. Additionally, without proper security setups, reviews can be difficult to complete, and take longer than preferred.


QUESTIONS???
D365UG | AXUG

Thank You!!!

Frank Vukovits
Fastpath, frank.Vukovits@gofastpath.com

Aaron Hamilton
Texas Roadhouse, aaron.hamilton@texasroadhouse.com