- Frank Vukovits
- Director – Strategic of Partnerships

Introduction

Frank Vukovits

- Director of Strategic Partnerships at Fastpath
- Certified Internal Auditor
- Certified Information Systems Auditor
- Twitter: @Fvukovits

Fastpath

- Founded in 2004
- Cloud-based Cross-Platform solution for Security, SoD, and Configuration management

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 Oracle.

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

GLOC
Great Lakes Oracle Conference

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
- 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

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 Oracle security
- Identify administrator access
- Choose a reviewer and a schedule
  - Business process owners vs. security admins
- Provide evidence of the review

In the Oracle, limited security reviews are often performed, because assignments were not documented originally, reviews are too time consuming, and reviews can be very manual.

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 Oracle World, security is often times an afterthought of the implementation or upgrade. Provisioning security, including roles, 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 Oracle World, often times the requesting and subsequent administration of security is burdensome. Takes a long time, 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

In the Oracle World, often times users are given System Administrator role access to help troubleshoot a problem, and that access is never turned back off.

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, as well, takes you outside of SoD review, but that is okay

In the Oracle, monitoring of security often times 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.


GLOC
Great Lakes Oracle Conference
Questions?
MAY 15 & 16, 2019
CLEVELAND PUBLIC AUDITORIUM, CLEVELAND, OHIO
WWW.NEOOUG.ORG/GLOC

THANK YOU

Frank Vukovits

frank.Vukovits@gofastpath.com

317.690.3483

www.gofastpath.com

GLOC
Great Lakes Oracle Conference