Demystifying Risk Management in ERPs

Andy Snook,
President, Fastpath
• Working together: audit + IT + business process owners
• Approaches to security and segregation of duties analysis
• Understanding systems and system access
• Automation & continuous monitoring
About Me

• President and founder of Fastpath, Inc.
• Certified in Risk and Information Systems Control
• 15 years experience in financial management systems
• 8 years experience in systems auditing
Fastpath Facts

- Founded 2004
- Headquarters in Des Moines, IA
- Microsoft Gold Competency ISV & ERP
- Staff includes CPAs and CIAs
Can we prove it?

- 800+ customers
- 30+ countries
- 6 continents
- IIA Industry Leader
Working Together Audit, IT and BPOs
Working Together Audit, IT and BPOs

• ERPs sit in the middle of IT and BPOs
• BPOs unsure of the underlying security
• IT unsure of the business process requirements/risks
• Few people have holistic view of process
  – Processing requirements
  – Financial
  – Roles
  – Systems, data, integrations
  – Risks
Working Together Audit, IT and BPOs

• Identify the processes that are in scope
• Use business process maps to unite the teams
• Involve audit, IT and BPOs in mapping
• Include roles, systems and risks in map
• Provides basis for documentation, training, auditing
Map the process

- Customer
- Salesperson
- Order Processing
- Customer Support
- AR Department
- Financial Systems Team
- Management Team
- Collections
- Microsoft Dynamics
- Order Admin
- Order Processing
- CRM

1. Customer Places Order
2. Is this a web order?
3. Enter Order Form info and attach contract
4. Receive email of new customer add/order
5. Validate order info and parameters
6. Setup user & accounts on website
7. Activate order. Send for invoice processing
8. Identify product line
9. Categorize orders for processing
10. Personal
11. Corp
12. Education

流程图：
- 顾客
- 销售员
- 订单处理
- 客户支持
- AR部门
- 财务系统团队
- 管理团队
- 收集
- 微软动态
- 订单管理
- 订单处理
- CRM
What does security and controls (S&C) mean?

“Security refers to the features around user application permissions whilst Controls refers to the process controls within and external to the application.

The goal is an environment that uses a blend of Security & Control measures to mitigate risks that are operational or financial in nature.”
Why is S&C Important?

- It will mitigate fraud and malicious activity
- Management decisions are based on accurate information
- Achieves process efficiencies (transforming manual into automated controls)
- Increases management confidence
- Compliance requirements (internal and external auditors)
What we see at our clients

• Access security is low priority for the project team
• Process controls are not part of the consideration
• Security design is the domain of IT/Sys Admin and business is not aware
• No on-going monitoring of process controls
• No consideration of segregation of duties
• Dilution of ‘go-live’ security design
• Inability to report on current security setup
• Expensive customisations in place of S&C features
Translate process and risk to ERP systems

• Base application security on business process maps
• Identify high risk business processes
• Determine functionality required for high risk processes
• Define risks, reviews, reviewers and periodicity
• Provide evidence that reviews are being done
An Excel spreadsheet of 1,000,000 rows
= **Forty** 3 ring binders of 500 pages each!

An excel sheet of 5,000 rows
= **One** 3 ring binder of 100 pages
Application Security – Who has access?

- Take a risk based approach
- Analyze by function not by user or risk
- Average system has over 5000 access points
- Average system has 30-40 high risk access points
- 500 vs. 1,000,000
- Reviews performed by BPOs not IT
Application Security – Who has access?

Customers
Vendors
Item/Inventory
Pricing
HR
Payroll
Process disbursements (check run)
Release/Approve purchase order
Goods receipt
Enter vendor invoices
Post journal entries
Open/Close GL accounts
Ship customer orders
Accounts Receivable transactions (post cash, credits)
Credit & Collection (credit limits, hold, release)
Customer order entry
Process/Modify customer invoices
Process credit memos
Write-off customer accounts
Record labor hours
Payroll payment (check run)
Prepare payroll (calculation/approval)
Open/Close Fiscal Periods
Maintain Users/User Security Privileges
System/Module Configuration - Settings
System access – Administrative Access

- What functions are required for admin
- Maintenance, code release, upgrades, security
- System admin role – how does it work?
  - Programmatic
  - Alternative – assign necessary (all?) roles to user
- Use named users with admin role
- Consultants use
- Periodic reviews
Application vs. Database Security

- How are they integrated?
- How are changes made at the database level?
  - Named users vs. Service account
- Periodic reviews
  - Reconcile app and db users
  - Administrative users
  - Custom integrations/outside access
Segregation of Duties

• Preventative vs. productivity
• Build a rule set of potential conflicts
• Identify Conflicts
• Mitigations
• 3 key questions
  – What are your rules?
  – Where are your risks?
  – What are you doing about it?
Audit trails – What did they do with that access?

• Take a risk based approach
  – Focus on key areas – Vendors, configuration, cash receipts, etc.
  – Focus on key fields – Payment terms, addresses, pricing, etc.

• Who changed it?

• When was it changed?

• Was it changed the right way?
Questions?

Andy Snook
snook@gofastpath.com
Twitter: @snookgofast